



香港銀行學會  
The Hong Kong Institute of Bankers

# Associate Operational Risk Management Professional (AORP)

<QF Level 4>\*

# Certified Operational Risk Management Professional (CORP)

<QF Level 5>#

## Programme Handbook

(Syllabus, Regulations and General Information)

AORP      CORP

\* The Professional Qualification "Associate Operational Risk Management Professional (AORP)" is recognised under the QF at Level 4. (QR Registration No: 21/001159/L4) (Validity Period from 01/11/2021 to 31/07/2025)

# The Professional Qualification "Certified Operational Risk Management Professional (CORP)" is recognised under the QF at Level 5. (QR Registration No: 21/001160/L5) (Validity Period from 01/11/2021 to 31/07/2025)

## Table of Contents

1. Introduction .....	3
2. Background.....	4
3. ECF on Operational Risk Management (Core Level) Programme Overview.....	8
3.1 Entry Requirements.....	8
3.2 Programme Objectives .....	8
3.3 Programme Intended Learning Outcomes .....	9
3.4 Learning Hours.....	9
3.5 Qualifications Framework.....	10
4. ECF on Operational Risk Management (Professional level) - Programme Overview .....	11
4.1 Entry Requirements.....	11
4.2 Programme Objectives .....	11
4.3 Programme Intended Learning Outcomes .....	11
4.4 Learning Hours.....	12
4.5 Qualifications Framework.....	12
5. Learning Support.....	13
6. Programme Syllabus .....	14
7. Training Application .....	56
8. Examination Application and Regulations.....	59
9. Certification Application and Renewal Process.....	68
10. Exemption Application and Regulations .....	71
10.1 Module Exemption Requirements .....	71
10.2 Module Exemption Application.....	72
11. General Information .....	73
11.1 Bad Weather Arrangements .....	73
12.2 Personal Data Protection Policy .....	74
12.3 Addendums and Changes .....	74
12. Contact information.....	75

# 1. Introduction

With the aim of supporting capacity building and talent development for banking professionals, the Hong Kong Monetary Authority (HKMA) has been working together with the banking industry to introduce an industry-wide competency framework - “**Enhanced Competency Framework (ECF) for Banking Practitioners**” in Hong Kong.

The Enhanced Competency Framework on Operational Risk Management (ECF on ORM) was introduced to develop a sustainable pool of operational risk management practitioners for the banking industry. The qualification structure of the ECF on ORM comprises two levels: Core Level and Professional Level, targeting entry level and junior level staff and staff taking up middle or senior positions in the operational risk management and business function risk and control.

As the programme and qualification provider of the ECF on ORM, The Hong Kong Institute of Bankers (HKIB) has developed the learning programme – the “**ECF on Operational Risk Management (ORM) (Core Level)**” to help individuals attain the Core Level of the competency standards set for the ECF on ORM. The programme “**ECF on Operational Risk Management (ORM) (Professional Level)**” helps individuals attain the Professional Level of the competency standards.

This Handbook provides programme details and relevant information for the learner who wants to complete the ECF on Operational Risk Management training and examination with the intent of obtaining the Professional Qualifications of “**Associate Operational Risk Management Professional (AORP)**” or “**Certified Operational Risk Management Professional (CORP)**”.

For more details, please refer to the HKMA’s Guide to ECF on Operational Risk Management at <https://www.hkma.gov.hk/media/eng/doc/key-information/guidelines-and-circular/2020/20201218e2.pdf> and HKIB website at <https://www.hkib.org/page/87>.

## 2. Background

### **A. Aims**

The aims of the ECF on Operational Risk Management are twofold:

- (i). To develop a sustainable talent pool of operational risk management practitioners for the banking industry; and
- (ii). To raise the professional competence of operational risk management practitioners in the banking industry.

### **B. Qualification Structure**

The competency standards of the ECF on Operational Risk Management comprise two levels: Core Level and Professional Level.

**Core Level** –This level is applicable to entry-level and junior level staff in the operational risk management and business function risk and control with 0-5 years of experience.

**Professional Level** –This level is applicable to staff taking up middle or senior positions in the operational risk management and business function risk and control with 5+ years of experience.

### **C. Scope of Application**

The ECF-ORM is intended to apply to staff whose primary responsibilities are performing operational risk governance, operational risk identification and assessment, operational risk monitoring and reporting, operational risk control and mitigation, and business resiliency and continuity planning within an AI.

Specifically, it is aimed at “Relevant Practitioners” (RPs) located in the Hong Kong office of an AI who perform the operational risk management job roles listed in the table below.

Job role of the ECF-ORM is stated below:

- (a) Role 1 – Operational Risk Management (i.e. staff in charge of managing operational risks in the second line of defence)

- i. Assist management in meeting their responsibility for understanding, monitoring and managing operational risks
  - ii. Develop and ensure consistent application of operational risk policies, processes, and procedures throughout the AI
  - iii. Ensure that the first line of defence activities are compliant with such policies through conformance testing
  - iv. Perform and assess stress testing and related scenario analysis
  - v. Provide training to and advise the business units on operational risk management issues
- (b) Role 2 – Business Function Risk and Control (i.e. staff working at the business units to manage operational risks in the first line of defence)
- i. Work within the first line of defence alongside management to be accountable for managing operational risk of business activities in the first line of defence
  - ii. Escalate operational risk events to senior management and operational risk management staff in the second line of defence, as required
  - iii. Work closely with operational risk management staff in the second line of defence to ensure consistency of policies and tools, as well as to report on results and issues
  - iv. Develop risk indicators, determine escalation triggers and provide management reports

For more details about the key tasks, please refer to the Annex 1 in HKMA's Guide to ECF on Operational Risk Management at <https://www.hkma.gov.hk/media/eng/doc/key-information/guidelines-and-circular/2020/20201218e2.pdf>

#### ***D. Certification and Public Register***

There are two Professional Qualifications under the ECF on ORM: Associate Operational Risk Management Professional (AORP), Certified Operational Risk Management Professional (CORP).

AORP: A Relevant Practitioner may apply to HKIB for the professional certification if he or she (1) has successfully completed all the three Core Level training modules (Modules 1 to 3) and obtained a pass in the relevant examination of each module or (2) has been grandfathered based on the required work experience upon the launch of the Core Level module.

CORP: A Relevant Practitioner may apply to HKIB for professional certification if he or she (1) has completed all the three Core Level training modules (Modules 1 to 3) and obtained a pass in the relevant examination of each module; (2) has successfully completed Module 4 of the Professional Level and passed the relevant examination plus five-year relevant experience in any of the functions as specified in Annex 1 stated in HKMA's "Guide to Enhanced Competency Framework on Operational Risk Management"; or (3) has been grandfathered based on the required work experience upon the launch of the Professional Level module. The five-year relevant work experience required for CORP certification should be accumulated within the ten years immediately prior to the date of application for certification, but it does not need to be continuous.

For details regarding grandfathering, please refer to [HKIB website](#) and the HKMA's [Guide to ECF on ORM](#).

By going through HKIB certification process successfully, the AORP/CORP holders are then registered as Certified Individuals (CI) and included in the public register on HKIB website. HKIB will also grant the AORP/ CORP holders a professional membership of HKIB.

**E. Annual renewal of certification and CPD Requirements**

Certifications of AORP/CORP are subject to annual renewal by HKIB. AORP/ CORP holders are required to meet the annual Continuing Professional Development (CPD) requirements and pay an annual certification fee to renew the certification.

For both the Core Level and Professional Level qualifications, a minimum of 12 CPD hours is required for each calendar year (ending 31 December). Out of the 12 CPD hours, at least six CPD hours must be earned from activities related to topics of compliance, legal and regulatory requirements, risk management and ethics. Any excess CPD hours accumulated within a particular year cannot be carried forward to the following year.




No CPD is required in the year when the AORP/ CORP Certification is granted. The CPD requirement starts in the following calendar year.

## 3. ECF on Operational Risk Management (Core Level)

### Programme Overview

#### 3.1 Entry Requirements

The Programme is open to members and non-members of HKIB. Candidates must fulfil the stipulated minimum entry requirements:

-  Students of Associate Degree (AD)/Higher Diploma (HD) in any disciplines (QF L4); OR
-  Equivalent qualifications or above; OR
-  Mature applicants<sup>1</sup> with either at least three years of work experience in banking and finance or equivalent with a recommendation from the employer.

#### 3.2 Programme Objectives

This programme has been developed with the aim to nurture a sustainable talent pool of operational risk management practitioners in the banking industry. Candidates will acquire technical skills, professional knowledge and conduct for entry-level and junior level of job roles in the risk management function that take up a majority of responsibility in operational risk management, business function risk and control.

---

<sup>1</sup> Mature applicants (aged 21 or above) who do not possess the above academic qualifications but with relevant banking experience and recommendation from their employers will be considered on individual merit.



### 3.3 Programme Intended Learning Outcomes

Upon completion of the programme, learners should be able to:

- ✚ Comply with business ethics and understand their place within modern financial institutions; understand ethical questions encountered in the second line of defence in the context of the broader risk environment
- ✚ Assess the regulatory landscape as per defined guidelines and procedures and identify operational risks encountered by different business units of the AI
- ✚ Apply the principles and methodologies of operational risk management for conducting operational risk monitoring duties according to the AI's policies and guidelines
- ✚ Analyse operational risks within different business units and effectively measure the likelihood and impact of such risks
- ✚ Apply appropriate techniques and requirements of operational risk assessments within different business units
- ✚ Understand the typical types of controls used in the banking industry
- ✚ Implement appropriate controls that effectively mitigate operational risks within different business units
- ✚ Examine operational risk matters and report to relevant stakeholders
- ✚ Analyse operational risk metrics and use operational risk reporting and dashboards to identify the potential operational risks

### 3.4 Learning Hours

The programme design is adopted a blended learning approach. For Module 1 and Module 2, learners are advised to spend not less than 100 Notional Learning Hours (equivalent to 10 credit). For Module 3, learners are advised to spend not less than 200 Notional Learning Hours (equivalent to 20 credit).

Notional learning time refers to the amount of time an average learner is expected to take to complete all learning pertaining to the programme, and achieve the learning outcomes expected.

It includes time spent on all learning modes and activities such as training class, self-study and assessment hours.

### **3.5 Qualifications Framework**

The Professional Qualification “Associate Operational Risk Management Professional (AORP)” is recognised under the QF at Level 4. (QR Registration No: 21/001159/L4) (Validity Period from 01/11/2021 to 31/07/2025)

Please refer to the [accreditation page](#) on HKIB website for more details.

## 4. ECF on Operational Risk Management (Professional level) -

### Programme Overview

#### 4.1 Entry Requirements

The Programme is open to members and non-members of HKIB. Candidates must fulfil the stipulated minimum entry requirements:

- ✚ Advanced Certificate for ECF on Operational Risk Management (ORM) awarded by HKIB;  
OR
- ✚ Grandfathered for ECF on Operational Risk Management (Core Level) by HKIB

#### 4.2 Programme Objectives

This programme has been developed with the aim to nurture a sustainable talent pool of operational risk management practitioners in the banking industry. Learners will acquire technical skills, professional knowledge and conduct for essential middle or senior level of job roles in the risk management function that take up a majority of responsibility in operational risk management, business function risk and control.

#### 4.3 Programme Intended Learning Outcomes

Upon completion of the programme, learners should be able to:

- ✚ Develop and establish operational risk management frameworks and associated policies and procedures
- ✚ Evaluate the operational risks encountered by different business units of the AI and establish effective mitigating controls
- ✚ Manage operational risks by using risk management control tools, e.g. risk control self-assessment (RCSA) and key risk indicators (KRIs)
- ✚ Develop risk control measures by using scenario analysis and stress testing to identify potential operational risk events and assess their potential impact
- ✚ Review the risk profile of the AI/business function and apply operational risk modelling to quantify and predict operational risks
- ✚ Compile the dashboards and metrics to measure and analyse operational risks within different business units
- ✚ Develop business continuity plan and recovery strategy

- ✚ Build and promote a risk focussed culture within the AI/within the business function
- ✚ Propose strategic operational risk advice and remedial actions to senior management on findings of operational risk events
- ✚ Design and deliver operational risk training to business units

#### **4.4 Learning Hours**

The programme design is adopted a blended learning approach. Learners are advised to spend not less than 300 Notional Learning Hours (equivalent to 30 credit). Notional learning time refers to the amount of time an average learner is expected to take to complete all learning pertaining to the programme, and achieve the learning outcomes expected. It includes time spent on all learning modes and activities such as training class, self-study and assessment hours.

#### **4.5 Qualifications Framework**

The Professional Qualification “Certified Operational Risk Management Professional (CORP)” is recognised under the QF at Level 5. (QR Registration No: 21/001160/L5) (Validity Period from 01/11/2021 to 31/07/2025)

Please refer to the [accreditation page](#) on HKIB website for more details.

## 5. Learning Support

### **HKIB Resources Corner Support**

The Resources Corner situated at the premises of HKIB provides the required learning resources required for study. Copies of the Recommended Readings are available in the Corner for borrowing. To provide updated learning resources to the members, HKIB has provided FREE internet and library service to the members.

Learners are encouraged to prepare the examination by acquiring relevant market information and module knowledge through various channels, e.g. reference readings, business journals, websites etc. Learners should be aware that such market information may be important and pertinent to the examinations.

### **Market Information Updates**

HKIB regularly organises training courses, seminars and luncheon talks on current issues and developments in financial markets that candidates may find essential, helpful and relevant to their learning.

## 6. Programme Syllabus

### Module 1: Ethics and Corporate Governance in Banking Industry

#### A. Module Intended Learning Outcome

Upon completion of this module, learners should be able to:

- ✚ Identify and apply the principles, requirements, and management of business ethical situations in the second line of defence in the context of broader risk environment encountered in the banking industry;
- ✚ Explain the organizational structures and exercise the requirement under the regulatory landscape in building an effective risk management framework to effective compliance;
- ✚ Identify different roles associated in building a culture for effective management of governance, risk, and compliance in financial institution;
- ✚ Apply regulatory requirement and effective compliance control on daily duties by demonstrating an understanding of and adopting the requirement related to corporate governance;

#### B. Syllabus

Chapter 1: Business Ethics	
1	- Introduction <ul style="list-style-type: none"> <li>• Introduction: Ethics and Law</li> </ul>
2	- Overview of Business Ethics <ul style="list-style-type: none"> <li>• What is Business Ethics</li> <li>• The importance of Business Ethics</li> <li>• Approaches to Normative Ethics: Absolutism and Relativism</li> </ul>
3	- Ethics and the Individual <ul style="list-style-type: none"> <li>• Code of Conduct:               <ul style="list-style-type: none"> <li>- Bank on Integrity</li> <li>- Conflict of Interest</li> <li>- Protecting Clients' Interests (Code of Banking Practice)</li> </ul> </li> <li>• Understanding Ethical Decision-making Process               <ul style="list-style-type: none"> <li>- The ETHICS-PLUS Decision-Making Model</li> <li>- CIMA – ETHICS Dilemmas Checklist</li> <li>- Ethics in Practice</li> </ul> </li> </ul>

<b>Chapter 2: Ethics and the Corporation</b>	
1	- Introduction <ul style="list-style-type: none"> <li>• Introduction: Corporate social responsibility, Corporate accountability and Corporate citizenship</li> </ul>
2	- Corporate Social Responsibility <ul style="list-style-type: none"> <li>• International Consensus</li> <li>• The pros and cons of implementing corporate social responsibility</li> <li>• The impact of Globalisation</li> </ul>
3	- Social Environmental Issues Facing Banks <ul style="list-style-type: none"> <li>• Environmental, Social Responsibility, Governance (“ESG”)</li> <li>• Equator Principles on Project Financing</li> <li>• Case study: “The Sustainability Report: The role of Bank on Sustainability”</li> </ul>
4	- Understanding Reputational Risk <ul style="list-style-type: none"> <li>• Key drivers of Reputation</li> <li>• Public Perception and Reputation Risk</li> <li>• Case studies: The Bank Runs</li> </ul>
<b>Chapter 3: Risk Management: Principles and Concepts</b>	
1	- Introduction <ul style="list-style-type: none"> <li>• Introduction: The importance of risk management as the key to effective compliance</li> </ul>
2	- Definition of Risk <ul style="list-style-type: none"> <li>• Definition of Risk</li> <li>• Different types of Risk in Banking (HKMA approach)</li> <li>• Other approaches to categorise risk</li> </ul>
3	- The Basic of Risk Management Framework <ul style="list-style-type: none"> <li>• Enterprise Risk Management Framework – the Three Lines of Defence</li> <li>• Key Elements of Effective Risk Management (ISO 31000: 2018 Risk Management Guideline)</li> <li>• The Three Lines of Defence (SPM IC-1 and Basel Requirement)</li> <li>• Organizational structure for an effective Risk Management Framework</li> </ul>
4	- An Overview of Key Risk Management Process <ul style="list-style-type: none"> <li>• Risk Identification</li> <li>• Risk measurement, analysis and evaluation</li> <li>• Risk monitoring and reporting</li> <li>• Risk mitigation</li> <li>• Methodologies and Governance of an Effective Risk Management Framework</li> </ul>

**Chapter 4: The Regulators, Law and Regulation**

- |   |  |
|---|--|
| 1 | <ul style="list-style-type: none"> <li>- Introduction           <ul style="list-style-type: none"> <li>• Introduction: The Prudential Approach</li> </ul> </li> </ul>  |
| 2 | <ul style="list-style-type: none"> <li>- Key Functions of Financial Regulators           <ul style="list-style-type: none"> <li>• The Hong Kong Monetary Authority (“HKMA”)</li> <li>• The Securities and futures Commission (“SFC”)</li> <li>• The Insurance Authority (“IA”)</li> <li>• The Mandatory Provident Fund Schemes Authority (“HPFSA”)</li> </ul> </li> </ul>  |
| 3 | <ul style="list-style-type: none"> <li>- Regulatory Requirements           <ul style="list-style-type: none"> <li>• An Overview:               <ul style="list-style-type: none"> <li>- Hong Kong Association of Banks</li> <li>- Code of Conduct – HKMA</li> <li>- Code of Conduct – SFC and SFO</li> <li>- The International Standard: Basel</li> </ul> </li> <li>• Know Your Customers / Due Diligence               <ul style="list-style-type: none"> <li>- Anti-money Laundering (“AML”) and Counter-Financing of Terrorism (“CFT”)</li> <li>- Sanction risk</li> <li>- Tax evasion and The Foreign Account Tax Compliance Act (“FATCA”)</li> <li>- Case studies: AML / CFT</li> </ul> </li> <li>• Suitability Obligations and Mis-selling               <ul style="list-style-type: none"> <li>- Suitability Obligations</li> <li>- Mis-selling claim</li> <li>- Case Study: Suitability Obligations and Mis-selling</li> </ul> </li> <li>• Market misconduct under the Securities and Futures Ordinance               <ul style="list-style-type: none"> <li>- Insider Trading</li> <li>- Price Rigging</li> <li>- Stock Market manipulation</li> <li>- Disclosure of Information about prohibited transaction (s. 276, s. 297)</li> <li>- Case Study: Mis-selling claim</li> </ul> </li> <li>• Protecting the Customers               <ul style="list-style-type: none"> <li>- Treat Customer Fairly Charter</li> <li>- Personal Data (Privacy) Ordinance                   <ul style="list-style-type: none"> <li>➤ Bank Marketing</li> <li>➤ Customer complaint management</li> <li>➤ Customers information management</li> </ul> </li> <li>- Case Study: Data Management in Banks</li> </ul> </li> </ul> </li> </ul> |



### Chapter 5: Corporate Governance in Banks

- |   |   |
|---|---|
| 1 | <ul style="list-style-type: none"> <li>- Introduction               <ul style="list-style-type: none"> <li>• What is Corporate Governance</li> <li>• Corporate Governance Principles for Banks (Basel Committee)</li> </ul> </li> </ul>   |
| 2 | <ul style="list-style-type: none"> <li>- Agency Theory               <ul style="list-style-type: none"> <li>• Agency theory</li> <li>• Agency costs</li> <li>• The public interest in financial stability                   <ul style="list-style-type: none"> <li>- The economic significance of banks</li> <li>- The unique business risks faced by banks</li> <li>- Systemic risk</li> </ul> </li> <li>• The misalignment between the interests of bank shareholders and the public interest</li> <li>• Case Study: Libor Manipulation and subsequent ethical ramification: the emergence of SOFR</li> </ul> </li> </ul>   |
| 3 | <ul style="list-style-type: none"> <li>- The Role and Composition of the Board               <ul style="list-style-type: none"> <li>• Structure of banks                   <ul style="list-style-type: none"> <li>- Organisational Structure</li> <li>- The Board</li> <li>- The Specialised committee</li> </ul> </li> <li>• Stakeholders in Corporate Governance</li> <li>• Regulatory Requirement and Implication                   <ul style="list-style-type: none"> <li>- HKMA CG-6 and ECF</li> <li>- SFC – Guideline on Competence</li> </ul> </li> </ul> </li> </ul>   |
| 4 | <ul style="list-style-type: none"> <li>- Accountability of Banks               <ul style="list-style-type: none"> <li>• Introduction                   <ul style="list-style-type: none"> <li>- Corporate Governance in Banking Industry under Basel requirement</li> <li>- Principle 12: Disclosure and transparency</li> </ul> </li> <li>• Disclosure                   <ul style="list-style-type: none"> <li>- Regulatory Accountability, Prudential Reporting and Regulatory Supervision</li> <li>- HKMA Supervisory Policy Manual – IC-2 (Internal audit Function)</li> </ul> </li> <li>• Transparency                   <ul style="list-style-type: none"> <li>- Introduction: Integrated Reporting</li> <li>- Environmental, Social and Governance Reporting</li> <li>- The International Integrated Reporting Committee Framework of Integrated Reporting</li> </ul> </li> </ul> </li> </ul> |

### Chapter 6: Remuneration and Appointment of Board Members, Chief Executive and Managers

- |   |  |
|---|--|
| 1 | - Introduction <ul style="list-style-type: none"> <li>• Introduction: The Competence of Board Directors and Chief Executive in Banks</li> </ul>  |
| 2 | - Principal Forms of Directorial and Executive Remuneration <ul style="list-style-type: none"> <li>• Basic Director's service fee</li> <li>• Executive salary</li> <li>• Bonus payments</li> <li>• Shares and restricted share grants</li> <li>• Executive share options</li> </ul>  |
| 3 | - Determination of Remuneration <ul style="list-style-type: none"> <li>• Fundamental principles: the guideline from Hong Kong Institute of Directors</li> <li>• The function of Remuneration committee</li> <li>• Determination of Non-executive Directors' remuneration</li> <li>• Guideline on a sound remuneration system (CG-5)</li> </ul> |
| 4 | - Appointments of Chief Executives and Directors <ul style="list-style-type: none"> <li>• Section 71 of Banking Ordinance</li> <li>• HKMA Requirements (CG-1, s. 6, 7)</li> </ul>  |
| 5 | - Appointments of Bank Managers <ul style="list-style-type: none"> <li>• Section 72B of Banking Ordinance</li> <li>• HKMA Requirements (CG-2, s. 3)</li> </ul>   |

### Chapter 7: Internal Control and Compliance in Banking

- |   |  |
|---|--|
| 1 | - Introduction <ul style="list-style-type: none"> <li>• Introduction: A Risk Based Approach to Bank Supervision (World Bank Paper Chp.15)</li> </ul>   |
| 2 | - The Elements of Internal Control System <ul style="list-style-type: none"> <li>• Elements of Internal Control System</li> <li>• Attributes of an effective control system</li> <li>• The Three Lines of Defence</li> </ul> |
| 3 | - Costs and Benefits of Internal Control <ul style="list-style-type: none"> <li>• Costs</li> <li>• Benefits</li> <li>• Case Study: Manipulation of US GSE debt securities trading before 2008</li> </ul>                     |
| 4 | - Second Line of Defence: The Compliance Function <ul style="list-style-type: none"> <li>• Regulatory Requirement (IC-1)</li> <li>• The Compliance functions</li> </ul>  |

5	<ul style="list-style-type: none"> <li>• The role of Compliance Officer</li> <li>- The Role of Risk Management Function to Effective Control and Compliance in Banks             <ul style="list-style-type: none"> <li>• The Voluntary Boundary</li> <li>• Core practice</li> <li>• Mandated boundary</li> <li>• Case Study: An example from Data Quality Management</li> </ul> </li> </ul>
---	--

### **C. Recommended Readings**

#### **Essential Readings**

1. HKIB Study Guide – Ethics and Corporate Governance in Banking Industry (2021)

#### **Supplementary Readings**

1. Mark Hsiao. (2013). Principles of Hong Kong Banking Law. Sweet & Maxwell
2. Iris H.-Y. Chiu, (2015). The Law of Corporate Governance in Banks. ISBN: 9781 78254 885 0

#### **Further Readings**

1. John R. Boatright. (2014). Ethics in Finance (3rd ed.). Wiley-Blackwell
2. Bessis, Joël. (2015) Risk Management in Banking. Fourth ed. Chichester, West Sussex: Wiley
3. Hong Kong Monetary Authority: Website and Supervisory Policy Manual
4. Securities and Futures Commission (2017). Code of Conduct for Persons Licensed by or Registered with the Securities and Futures Commission
5. ISO 31000: 2018 Risk management Guidelines

## **Module 2: Regulatory Framework and Compliance in Banking Industry**

### **A. Module Intended Learning Outcome**

Upon completion of this module, learners should be able to:

- ✚ Understand and explain the role and function of financial regulatory framework specifically the role of the HKMA and various other regulators including SFC and IA in regulating the banking industry;
- ✚ Describe and apply the Banking Ordinance and other relevant laws applicable to banks, as well as the HKMA statutory guidelines and guidance notes, in the day to day running of various businesses of a bank;
- ✚ Design and implement systems and controls for banks to ensure all legal and regulatory requirements are satisfied;
- ✚ Assess compliance related operational risk indicators, assessment of the risks and based on the legal and regulatory requirement, develop strategies to mitigate the risks maintaining compliance position of the bank at the tolerance level;
- ✚ Monitor and identify problems and issues in various banking businesses and making informed judgement and propose solutions in compliance with all the legal and regulatory requirements

### **B. Syllabus**

<b>Chapter 1: Overview of Regulatory Regime for Bank in Hong Kong</b>	
1	- Introduction
2	- Overall Financial Regulatory Framework in Hong Kong
3	- Hong Kong Monetary Authority – Regulatory Framework
4	- Securities and Futures Commission – Regulatory Framework
5	- Insurance Authority – Regulatory Framework
6	- Mandatory Provident Fund Scheme Authority – Regulatory Framework
7	- Hong Kong Monetary Authority – The Lead Regulator of Bank
<b>Chapter 2: Banking Supervision, Internal Polices, Standards and Guidelines</b>	
1	- Introduction
2	- Supervisory Approach and CAMEL Rating
3	- Risk-Based Supervisory Approach
4	- Hong Kong Monetary Authority and Hong Kong Exchanges and Clearing Limited – Corporate Governance Requirements
5	- Risk Management System of Als
6	- Regulatory Expectation of Internal Controls System

<b>Chapter 3: Bank Culture Reform</b>	
1	- Introduction
2	- Treat Customers Fairly Charter (2013)
3	- Bank Culture Reform Circular (2017)
4	- Supervisory Measures for Bank Culture
5	- Self-assessment on Bank Culture Reform
6	- Focus Review, Culture Dialogue and Industrial Survey
<b>Chapter 4: Major Statutory Requirements for Bank in Hong Kong</b>	
1	- Introduction
2	- Banking Ordinance
3	- Securities and Futures Ordinance
4	- Insurance Ordinance
5	- Mandatory Provident Fund Schemes Ordinance
6	- Personal Data (Privacy) Ordinance
<b>Chapter 5: Regulatory Objectives and Relevant Mandates</b>	
1	- Introduction
2	- Code of Banking Practice
3	- Code of Conduct for Persons Licensed by or Registered with the Securities and Future Commission
4	- Code of Conduct for Licensed Insurance Agents and Code of Conduct for Licensed Insurance Brokers
5	- Guidelines on Conduct Requirements for Registered Intermediaries (Issued by the Mandatory Provident Fund Schemes Authority)
<b>Chapter 6: Introduction to International Regulation</b>	
1	- Introduction
2	- International Regulations (Role of Regulators, Regulatory Powers and International Regulatory Models and Latest Market Trends)
3	- FATCA
4	- Common Reporting Standards (AEOI/CRS)
5	- EU General Data Protection Regulation (GDPR)
<b>Chapter 7: Registration and Licensing Requirements</b>	
1	- Introduction
2	- Banking Ordinance – AI, CE, ACE and Manager
3	- Securities and Futures Ordinance – Registered Institution and Relevant Individual
4	- Insurance Ordinance – Agency and Technical Representative
5	- Mandatory Provident Fund Schemes Ordinance – MPF Intermediary

6	- Listing Rules – Listed AIs
7	- Manager-in-charge (MIC) Regime – Applicability to AIs
<b>Chapter 8: Regulatory Breach and Operational Risk Incident Management</b>	
1	- Introduction
2	- Identification, Review and Classification of Incident
3	- Response and Management of Operational Risk Incident – Internal Escalation
4	- Response and Management of Operational Risk Incident - Remediation and Disclosure
5	- Response and Management of Operational Risk Incident - Lesson Learnt and System Enhancement
6	- Operational Risk Incident Regulatory Reporting Requirement of the HKMA
7	- Reputational Issue in Incident Management
<b>Chapter 9: Future Development in Banking and the Relevant Regulatory Requirements</b>	
1	- Introduction
2	- Digital Banking and e-Banking Regulatory Requirements
3	- Open API and Open Banking Development in Hong Kong
4	- Virtual Banking Licensing and Regulatory Development
5	- Sustainable and Green Banking Business Development in Hong Kong
6	- Regulatory and Compliance Challenges from Sustainable and Green Banking Business
<b>Chapter 10: Case Studies – Compliance Challenge</b>	
1	- Introduction
2	- Challenge of New Products and Services
3	- Challenge of Ongoing Changes in Regulatory Requirements
4	- Challenge of External Event
5	- Case Study – Compliance Breach involving Staff Misconduct
6	- Case Study – Operational Risk Incident with Major Customer Impact

### **C. Recommended Readings**

#### **Essential Readings**

1. HKIB Study Guide – Regulatory Framework and Compliance in Banking Industry (2021)

#### **Supplementary Readings**

1. Hong Kong Legislation – Chapter 155, Chapter 571, Chapter 41, Chapter 485 and Chapter 486.

2. Hong Kong Monetary Authority- Supervisory Policy Manual (2001) Risk-based supervisory approach
3. Hong Kong Monetary Authority- Supervisory Policy Manual (2017) Corporate governance of locally incorporated authorized institutions
4. Hong Kong Monetary Authority- Supervisory Policy Manual (2017) Risk Management Framework
5. Hong Kong Monetary Authority- Supervisory Policy Manual (2018) Interest Rate Risk in the Banking Book
6. Hong Kong Monetary Authority- Supervisory Policy Manual (2005) Operational risk management
7. Hong Kong Monetary Authority- Supervisory Policy Manual (2003) General principles for technology risk management
8. Hong Kong Monetary Authority- Supervisory Policy Manual (2001) General principles of credit risk management
9. Hong Kong Monetary Authority- Circular (2013) on Bank Culture Reform
10. The Hong Kong Association of Banks/The DTC Association - (2015) Code of Banking Practice
11. Securities and Futures Commission - (2020) Code of Conduct for Persons Licensed by or Registered with the Securities and Futures Commission
12. Insurance Authority – (2019) Code of Conduct for Licensed Insurance Agents
13. Competition Commission – (2015) Guideline on the First Conduct Rule and Guideline on the Second Conduct Rule

**Further Readings**

1. Beecham, B.J., 2003 Monetary and Financial System in Hong Kong 3rd Edition. Hong Kong Institute of Bankers 2003

## **Module 3: Fundamentals of Operational Risk Management and Risk Governance**

### **A. Module Intended Learning Outcome**

Upon completion of this module, learners should be able to:

- ✚ Understand the objectives and the types of Operational Risk Management;
- ✚ Establish solid operational risk governance, define clear roles and responsibilities and support risk culture in the organization;
- ✚ Apply and practice the operational risk principles and define the operational risk appetite;
- ✚ Execute the operational risk assessment, measurement and reporting;
- ✚ Understand and integrate with technology, resiliency and enterprise risk assessment

### **B. Syllabus**

<b>Chapter 1: Overview of Operational Risk</b>	
1	- Introduction
2	- Definitions <ul style="list-style-type: none"> <li>• Definition of Risk Management</li> <li>• Importance of Risk Management</li> <li>• Types of Operational Risks faced by the Bank</li> <li>• Taking Risk as Integral Part of Banking</li> <li>• Definition and Types of Inherent Risks</li> <li>• CAMEL Process</li> <li>• Risk Management System</li> <li>• Risks in Banking and Financial Services</li> <li>• Evolution of Operation Risk</li> <li>• Business Lines of the Banking Industry</li> <li>• Definition of Risk (ISO 31000)</li> <li>• Difference between Certainty VS Risk VS Uncertainty</li> <li>• Definition of Operational Risk</li> <li>• Operations Risk VS Operational Risk</li> <li>• Inherent Risk VS Residual Risk</li> <li>• Preview on Top 10 Operational Risks</li> <li>• Top Operational Risk Issues Discussed in Board Room</li> <li>• Operational Risk Management Framework</li> </ul>
3	- Drivers <ul style="list-style-type: none"> <li>• Benefits of Operational Risk Management</li> <li>• Value of Operational Risk Management</li> </ul>



	<ul style="list-style-type: none"> <li>• Key Deliverables of Sound Operational Risk Management</li> <li>• Drivers of Good Operational Risk Management</li> <li>• Lesson Learnt on Drivers Leading to 2008 Financial Crisis</li> <li>• Reasons Leading to Management of Operational Risk</li> <li>• Key Internal Operational Risk Drivers</li> <li>• Categories of Operational Risk Drivers</li> <li>• Operational Risk Causal Factors</li> <li>• Process Factors</li> <li>• People Factors</li> <li>• System Factors</li> <li>• External Factors</li> <li>• Other Specific Operational Risk Drivers – Culture and Strategy</li> <li>• Other Specific Operational Risk Drivers – Regulators and M&amp;A</li> <li>• Other Specific Operational Risk Drivers – Best Practice and Risk Aggregation</li> <li>• Other Specific Operational Risk Drivers – New Products and Performance &amp; Resource Allocation</li> <li>• Expectation from Stakeholders</li> <li>• Use of Operational Risk in Decision Making</li> <li>• Positioning Operational Risk as Business Enabler</li> </ul>
4	<p>- Different Types</p> <ul style="list-style-type: none"> <li>• Risk Taxonomy</li> <li>• Topology of Financial Risks</li> <li>• Basel Level of Categorisation of Operational Risk</li> <li>• Basel Categories of Business Lines</li> <li>• Basel Categories of Event Types</li> <li>• Typical Types Operational Risks</li> <li>• Current Market Development that Requires Risk Attention</li> <li>• Factors Leading to Operational Risk Vulnerabilities</li> <li>• Samples of Major Prominent Operational Risk Events by Business Functions</li> <li>• Iceberg Model</li> </ul>
5	<p>- Risk Analysis Model – Cause, Events, Impact</p> <ul style="list-style-type: none"> <li>• Swiss Cheese Model</li> <li>• Operational Risk Event and Causal Effects</li> <li>• ORX Extended Causes and Impact Model</li> <li>• ORX Operational Loss Industry Pattern</li> <li>• ORX Extended Causes and Impact Model</li> <li>• ORX Causes Categories</li> <li>• ORX Event Categories</li> </ul>

6	-	<ul style="list-style-type: none"> <li>• ORX Impact Categories</li> <li>• Risk Management Sequence</li> <li>- Relationship with Other Risk Functions <ul style="list-style-type: none"> <li>• Recap on Risks in Bank</li> <li>• Linkage of Different Risks to the Risk Event and Impact</li> <li>• Boundaries of Operational Risk</li> <li>• Structural Differences between Risk Types</li> <li>• Risk Relationships and Interconnectivity</li> <li>• Risk Boundaries – Operational Risk and Credit Risk Examples</li> <li>• Risk Boundaries – Operational Risk and Market Risk Examples</li> <li>• Differences between Operational Risk and other types of risks</li> <li>• Identification – Unit of Measure</li> <li>• Quantification / Measurement</li> <li>• Mitigation / Control</li> <li>• Comparisons between Operational Risk, Market Risk, and Credit Risk Management</li> <li>• Integrating Related Disciplines in Banks</li> <li>• Good Risk DNA</li> </ul> </li> </ul>
7	-	<ul style="list-style-type: none"> <li>- Case Studies <ul style="list-style-type: none"> <li>• Case Study: Unauthorized Trading</li> <li>• Case Study: Staff Embezzlement</li> <li>• Case Study: G17reach of Fiduciary Duties</li> <li>• Case Study: Leakage of Customer Data</li> <li>• Case Study: Letters of Credit Card Fraud</li> <li>• Case Study: Top 10 Operational Loss Cases 2019</li> <li>• Case Study: Top 10 Operational Loss Cases 2018</li> <li>• Case Study: Top 10 Operational Loss Cases 2017</li> </ul> </li> </ul>
8	-	<ul style="list-style-type: none"> <li>- Best Practice Guidance <ul style="list-style-type: none"> <li>• Use of Risk Exposure Indicators</li> <li>• Risk Management Adoption Maturity Model</li> <li>• Looking Forward Risk Radars</li> </ul> </li> </ul>
<b>Chapter 2: Operational Risk Framework and Governance</b>		
1	-	Introduction
2	-	<ul style="list-style-type: none"> <li>- Risk Governance Structure <ul style="list-style-type: none"> <li>• Operational Risk Management Framework</li> <li>• Key Recent Regulatory Changes (CG-1, IC-1)</li> <li>• HKMA Revision to Risk Management Module IC-1</li> <li>• Elements of a Sound Risk Management System</li> <li>• General Components of Operational Risk Framework</li> </ul> </li> </ul>

	<ul style="list-style-type: none"> <li>• ORM Frameworks and Goals</li> <li>• Corporate Governance</li> <li>• Operational Risk Governance</li> <li>• Typical Operational Risk Governance Structure Diagram</li> <li>• Risk Culture and Operational Risk Governance</li> <li>• Operational Risk Leadership</li> <li>• Modes of Accountability</li> </ul>
3	<ul style="list-style-type: none"> <li>- Three Lines of Defence           <ul style="list-style-type: none"> <li>• Three Lines of Defense</li> <li>• Responsibilities of Three Lines of Defense</li> <li>• Evolution of 1.5 Line</li> <li>• Three Lines of Defence Approach</li> <li>• An Alternative 'Blended' Approach</li> <li>• Three Lines of Defence Partnership Model</li> </ul> </li> </ul>
4	<ul style="list-style-type: none"> <li>- Roles and Responsibilities           <ul style="list-style-type: none"> <li>• Roles and Responsibilities</li> <li>• Role of Board and Senior Management</li> <li>• Role of Business and Support Units – 1st LOD</li> <li>• Role of Corporate Operational Risk Function (CORF) – 2nd LOD</li> <li>• Role of Corporate Subject Matter Specialists – Part of 2nd LOD</li> <li>• Communication, Consultation and Collaboration Among the Three Lines</li> <li>• Operational Risk Committee</li> <li>• Points of Escalation to Various Committees</li> </ul> </li> </ul>
5	<ul style="list-style-type: none"> <li>- Risk Culture and Indicators           <ul style="list-style-type: none"> <li>• Definition of Risk Culture</li> <li>• Levels of Risk Culture</li> <li>• Risk Sub-Culture</li> <li>• Assessing Risk Culture</li> <li>• Definition of Operational Risk Culture</li> <li>• Attitudes, Behaviours and Culture</li> <li>• Importance of Risk Culture</li> <li>• Risk Culture (Principle 1 of PSMOR)</li> <li>• Risk Culture Aspects Model</li> <li>• Some Indicators of Good Risk Culture</li> <li>• Monitoring Risk Culture: Risk Culture Metrics</li> <li>• Monitoring Risk Culture: Risk Culture Metrics - Example</li> <li>• Influencing Risk Culture</li> <li>• Implication on Strategy and Leadership (Including Tone)</li> </ul> </li> </ul>

6	<ul style="list-style-type: none"> <li>• Implication on Risk Appetite and Tolerance</li> <li>• Implication on HR Policies and Procedures</li> <li>• Implication on Communication: Formal and Informal</li> <li>• Implication on Process and System Design</li> <li>• Implication on Risk Governance</li> <li>• Reflection on HKMA Bank Culture Self Assessment</li> </ul> <p>- Risk Governance on Handling of Emerging Risk</p> <ul style="list-style-type: none"> <li>• Definition of Emerging Risks</li> <li>• Interconnection of Risks</li> <li>• Typology of Uncertainties</li> <li>• Types of Emerging Risk</li> <li>• ORX 2019 Top Emerging Risks</li> <li>• Emerging Risk Trend</li> <li>• Emerging Risk Radar</li> <li>• Projection of Emerging Top Risks</li> <li>• Emerging Risk – Cyber Risk</li> <li>• Emerging Risk – Emerging Technology</li> <li>• Emerging Risk – Climate Risk Hazards</li> <li>• Emerging Risk Framework</li> <li>• Drivers of Emerging Operational Risks</li> <li>• Contributing Factors to Emerging Operational Risk</li> <li>• Governance of Emerging Risk</li> <li>• Risk Biases Leading to Hidden Emerging Risks</li> <li>• Identification of Emerging Risks and Opportunities</li> <li>• Tools for Identification of Emerging Risks</li> <li>• Increasing Awareness of Potential Risks</li> <li>• Risk Velocity</li> <li>• Action on Emerging Risk</li> <li>• Solution to Overcome Risk Biases</li> </ul>
7	<p>- Case Studies</p> <ul style="list-style-type: none"> <li>• Case Study: Misappropriation of an AI's money by a staff member</li> </ul>
8	<p>- Best Practice Guidance</p> <ul style="list-style-type: none"> <li>• Building Blocks of Operational Risk Culture</li> <li>• Embedding Risk in Business Strategy</li> </ul>
<b>Chapter 3: Operational Risk Principles and Appetite</b>	
1	<p>- Introduction</p>
2	<p>- Principles of Operational Risk Management Framework and Implementation</p> <ul style="list-style-type: none"> <li>• Basel Consultative Paper – Revisions to Principles for the Sound Management of</li> </ul>

		Operational Risk (PSMOR)
		<ul style="list-style-type: none"> <li>• Structure of Principles for the Sound Management of Operational Risk</li> <li>• Key Objectives of Operational Risk Principles</li> <li>• Summary of the 12 Basel PSMOR</li> <li>• Role of Supervisors</li> <li>• Deep Dive on Operational Risk Framework (Principle 2 of PSMOR) - Framework</li> <li>• Deep Dive on Operational Risk Framework (Principle 3 of PSMOR) - Governance</li> <li>• Principles for Effective Risk Management (ISO 31000)</li> <li>• Stages of ORM Implementation in Banks</li> </ul>
3	-	<p>Risk control and mitigation</p> <ul style="list-style-type: none"> <li>• Definition of Internal Controls</li> <li>• Deep Dive on Control and Mitigation (Principle 9 of PSMOR)</li> <li>• HKMA Requirement on Internal control System</li> <li>• Internal Control Model</li> <li>• Several Typical Operational Risks in Business Processes and the Related Control Measures</li> <li>• Internal Control System</li> <li>• Types of Internal Controls</li> <li>• Definition of Control Testing</li> <li>• Types of Internal Control Testing</li> <li>• Risk Based Internal Control Testing</li> <li>• Active Failures and Latent Conditions</li> <li>• Effect of Internal Controls on Risks</li> <li>• Effectiveness of Controls</li> </ul>
4	-	<p>Operational Risk Planning and Processes</p> <ul style="list-style-type: none"> <li>• Operational Risk Planning</li> <li>• Overview of Operational Risk Management Process</li> <li>• Operational Risk Management Process</li> <li>• Operational Risk Management Process-Broad Steps</li> <li>• Operational Risk Management Actions and Tools</li> <li>• The Bow Tie Diagram</li> <li>• Operational Risk Event, Cause and Effect</li> <li>• “Swiss Cheese” Model of Defences</li> </ul>
5	-	<p>Operational Risk Appetite Framework</p> <ul style="list-style-type: none"> <li>• Definition of Operational Risk Appetite</li> <li>• Benefits of Operational Risk Appetite</li> <li>• Focus of Operational Risk Appetite</li> <li>• Operational Risk Tolerance</li> </ul>

	<ul style="list-style-type: none"> <li>• Determination of Operational Risk Appetite and Risk Tolerance</li> <li>• The R&amp;R of the Board on the Determination</li> <li>• The R&amp;R of the Business Management on the Determination</li> <li>• The R&amp;R of the Internal Audit on the Determination</li> <li>• Diagrammatic Explanation of Risk Appetite Funnel</li> <li>• Top-down and Bottom-up Approaches to Setting the Appetite</li> <li>• Alignments of the Frameworks to the Different Forms of Risk Appetite Expression</li> <li>• Expressing the Operational Risk Appetite (ORA) Quantitatively and Qualitatively</li> <li>• Deciding on the Appropriate Level of the ORA and Risk Tolerances</li> <li>• Implementing the ORA and Tolerances</li> <li>• Aggregation and Reporting</li> <li>• Management and Decision Making</li> <li>• Sample Operational Risk Appetite Template</li> <li>• Structure of Actionable Risk Appetite</li> <li>• Consistent Operational Risk Appetite</li> <li>• Articulating Operational Risk Appetite</li> <li>• Defining Operational Risk Appetite</li> <li>• Setting Operational Risk Appetite and Tolerance</li> <li>• Setting Operational Risk Appetite Thresholds</li> <li>• Setting and Application</li> <li>• Market View on Operational Risk Appetite</li> <li>• Operational Risk Assessment for New Business, Product, and Changes</li> <li>• Operational Risk Heatmap</li> <li>• Background, Methodology, and Deliverables of the Critical Operational Risk Registers</li> <li>• Examples of Operational Risk Appetite Statements</li> </ul>
6	- Operational Risk Impact <ul style="list-style-type: none"> <li>• Developing Assessment Criteria</li> <li>• Sample of Operational Risk Rating Scale</li> <li>• ORX Impact Categories</li> </ul>
7	- Case Studies <ul style="list-style-type: none"> <li>• Case Study: Ineffective Call-back Verification on Third-party Fund Transfers</li> </ul>
8	- Best Practice Guidance <ul style="list-style-type: none"> <li>• Best Practice Principles on Operational Risk Appetite</li> <li>• Internal Controls (Control Environment and Business Process Controls)</li> <li>• Interaction between Operational Risk Management Tools</li> <li>• Operational Risk Management Tools Metrics</li> </ul>
<b>Chapter 4: Operational Risk Assessment, Measurement And Reporting</b>	
1	- Introduction

2	<ul style="list-style-type: none"> <li>- Operational Risk Assessment           <ul style="list-style-type: none"> <li>• Stages of Operational Risk Assessment Process</li> <li>• Methods for Assessing Risks</li> <li>• Identifying Operational Risk</li> <li>• Tools of Operational Risk Assessment</li> <li>• Benchmarking for Identification</li> <li>• Risk Factors for Consideration</li> <li>• HKMA Requirement on Operational Risk Assessment Methods</li> </ul> </li> </ul>
3	<ul style="list-style-type: none"> <li>- Quantification of Operational Risk           <ul style="list-style-type: none"> <li>• Explanation of Quantification of Operational Risk</li> <li>• Value at Risk (VaR)</li> <li>• Conditional VaR</li> <li>• Extreme Value Theory</li> <li>• Peaks-over-Threshold</li> <li>• Fuzzy Logic</li> <li>• Bayesian Belief Network</li> <li>• Artificial Neural Networks</li> <li>• Bootstrapping</li> <li>• Heat Map</li> <li>• Risk Registers</li> <li>• Practical Consideration</li> </ul> </li> </ul>
4	<ul style="list-style-type: none"> <li>- Risk Reporting and Dashboard           <ul style="list-style-type: none"> <li>• Objectives of Operational Risk Reporting</li> <li>• Factors of Operational Risk Reporting</li> <li>• Process of Operational Risk Reporting</li> <li>• Typical Contents of Operational Risk Reports</li> <li>• Timeliness of Operational Risk Reports</li> <li>• Features of Operational Risk Reporting</li> <li>• Types of Operational Risk Reporting</li> <li>• Action of Operational Risk Reporting</li> <li>• Best Practice Principles of Operational Risk Reporting</li> <li>• Critical Success Factors of Operational Risk Reporting</li> <li>• Examples of Operational Risk Reports</li> <li>• Checkpoints on Good Operational Risk Reporting</li> </ul> </li> </ul>
5	<ul style="list-style-type: none"> <li>- Nature of The Financial Products           <ul style="list-style-type: none"> <li>• Overview of Financial Service Products</li> <li>• Funds Intermediation Products</li> <li>• Transaction Intermediation Products</li> </ul> </li> </ul>

	<ul style="list-style-type: none"> <li>• Information Intermediation Products</li> <li>• Risk Intermediation Products</li> <li>• Work Activity Related to Financial Services Products</li> <li>• Managing Risk in New Product Development</li> <li>• Key Features of Equity</li> <li>• Demonstrate Understanding of Equity</li> <li>• Key Features of Various Types of Bonds</li> <li>• International Bond Markets</li> <li>• Major Categories of Money Market Products</li> <li>• Differences and Similarities between the Major Types of Cash Money Market</li> <li>• The Major Commodity Categories</li> <li>• Major Categories of Derivative Products</li> <li>• The Markets where Major Categories of Derivative Products Are Usually Traded</li> <li>• Major Categories of Alternative Investments</li> </ul>
6	<ul style="list-style-type: none"> <li>- Common Risk Types <ul style="list-style-type: none"> <li>• Types of Operational Loss</li> <li>• Types of Categorization of Operational Risk</li> <li>• Rationale for Operational Risk Categorisation</li> <li>• Key Principles for Categorising Operational Risks</li> <li>• Designing an Operational Categorisation Framework</li> <li>• Minimising Gaps and Overlaps</li> <li>• Improving Granularity</li> <li>• Implementation – Roles and Responsibilities</li> <li>• Implementation – Ensuring Consistent Use</li> <li>• Implementation – Reporting</li> <li>• Implementation – Addressing Boundary Events</li> <li>• Common Risk Types of Services and Products</li> <li>• Typology of Operational Risks</li> </ul> </li> </ul>
7	<ul style="list-style-type: none"> <li>- Case Studies <ul style="list-style-type: none"> <li>• Case Study: Mistake in Allowing an Authorized Person to Bring in Another Person when Accessing a Safe</li> </ul> </li> </ul>
8	<ul style="list-style-type: none"> <li>- Best Practice Guidance <ul style="list-style-type: none"> <li>• Theme and Metrics for Conduct Risk Reporting</li> <li>• Example of Conduct Risk Metrics Reporting</li> </ul> </li> </ul>
<b>Chapter 5: Technology, Resiliency And Enterprise Risk Assessment</b>	
1	<ul style="list-style-type: none"> <li>- Introduction</li> </ul>
2	<ul style="list-style-type: none"> <li>- Technology Risk Framework <ul style="list-style-type: none"> <li>• Operational Risk in Information Technology</li> </ul> </li> </ul>



3	<ul style="list-style-type: none"> <li>• Regulations for Technology Management in Banking Industry</li> <li>• Managing Information and Communication Technology</li> <li>- Cybersecurity <ul style="list-style-type: none"> <li>• Typology of Information Security Risk</li> <li>• Types of Cyber Security Threats</li> <li>• Sample of Information Security Risk Assessment</li> <li>• Key Controls in Information Security</li> <li>• Sample of KRI in Information Security</li> <li>• Cybersecurity Standards</li> <li>• Information Security Management System</li> <li>• ISO/IEC 27001 Information Security Management Systems Standard</li> <li>• Sharing of Cyber-threat Information</li> <li>• Principal Cyberactivities that are Criminalised by the Law</li> <li>• Information Security Challenges Associated with Cloud Computing</li> <li>• Cybersecurity Laws Affect Foreign Organisations</li> <li>• Additional Cybersecurity Protections Beyond What Is Mandated by Law</li> <li>• Government Incentivize Organizations to Improve Their Cybersecurity</li> </ul> </li> </ul>
4	<ul style="list-style-type: none"> <li>- Data Privacy <ul style="list-style-type: none"> <li>• Overview of Data Privacy</li> <li>• Regulation on Data Privacy PDPO and HKMA SPM TM-E-1</li> </ul> </li> </ul>
5	<ul style="list-style-type: none"> <li>- System Change Control <ul style="list-style-type: none"> <li>• Risk Management in Change</li> <li>• Quality Assurance, Testing, and Change Management</li> </ul> </li> </ul>
6	<ul style="list-style-type: none"> <li>- Resiliency Risk <ul style="list-style-type: none"> <li>• Definition of Resiliency</li> <li>• Threats to Financial Resilience</li> <li>• Interconnects of Financial and Operational Resiliency</li> <li>• Drivers of Operational Resilience</li> <li>• Risk, Resilience and Sustainability</li> <li>• Managing Business Continuity Planning</li> <li>• Business Continuity Management</li> </ul> </li> </ul>
7	<ul style="list-style-type: none"> <li>- Types of Disasters <ul style="list-style-type: none"> <li>• Types of Disasters</li> <li>• Classification of Disasters</li> <li>• Disasters VS Catastrophes</li> </ul> </li> </ul>
8	<ul style="list-style-type: none"> <li>- Business Impact Analysis <ul style="list-style-type: none"> <li>• Definition of Business Impact Analysis</li> <li>• Analysis of Business Impact Analysis</li> </ul> </li> </ul>

9	-	<ul style="list-style-type: none"> <li>• Business Impact Analysis VS Risk Assessment</li> <li>• HKMA Requirement on Business Impact Analysis</li> </ul>
	-	Resiliency Plan
	-	<ul style="list-style-type: none"> <li>• Definition of Business Continuity</li> <li>• Roles and Responsibilities of Business Continuity Management</li> <li>• Components of Business Continuity Management</li> <li>• BCM Lifecycle</li> <li>• Contingency Planning</li> </ul>
10	-	Plan Testing
	-	<ul style="list-style-type: none"> <li>• HKMA Requirement on Contingency Planning Testing</li> <li>• HKMA Requirement on Contingency Planning Maintenance</li> </ul>
11	-	Enterprise Risk Framework
	-	<ul style="list-style-type: none"> <li>• Overview of Enterprise Risk Management</li> <li>• Definition of Enterprise Risk Management</li> <li>• HKMA Requirement on Firm-wide Risk Management</li> <li>• COSO Enterprise Risk Management Framework</li> <li>• New COSO ERM - Integrating with Strategy and Performance</li> <li>• Capability of Enterprise Risk Management</li> <li>• Key Elements of an Effective Operational Risk within ERM Framework</li> <li>• Integration of ORM Framework into ERM</li> </ul>
12	-	Enterprise Risk Appetite
	-	<ul style="list-style-type: none"> <li>• Enterprise Risk Appetite</li> <li>• Roles and Responsibilities in Risk Appetite Framework</li> <li>• HKMA Requirement on Enterprise Risk Appetite Framework</li> </ul>
13	-	Enterprise Risk Limit
	-	<ul style="list-style-type: none"> <li>• Enterprise Risk Limit</li> <li>• Best Practice on Enterprise Risk Limit</li> <li>• Structure on Enterprise Risk Limit</li> <li>• HKMA Requirement on Enterprise Risk Limit</li> </ul>
14	-	Case Studies
	-	<ul style="list-style-type: none"> <li>• Case Study: Misappropriation of a Customer's Funds by a Staff Member Using a Returned ATM Card</li> </ul>
15	-	Best Practice Guidance
	-	<ul style="list-style-type: none"> <li>• The Main Industry Standards and Codes of Practice Promoting Cybersecurity (HKMA, SFC, IA, OGCIO, PCPD)</li> </ul>
<b>Chapter 6: Integrated Case Studies And Best Practices</b>		
1	-	Integrated Case Studies
	-	<ul style="list-style-type: none"> <li>• Case Study: The Collapse of Barings Bank 1995</li> </ul>

2	- <ul style="list-style-type: none"> <li>• Case Study: Safety Deposit Boxes at DBS</li> <li>• Case Study: Société Générale Taken to the Brink</li> <li>• Lesson Learnt</li> <li>• Best Practice Guidance</li> <li>• Ten Principles of the Best Practices in ORM</li> </ul>
---	--

### **C. Recommended Readings**

#### **Essential Readings**

1. Ariane Chapelle (2018). Operational Risk Management: Best Practices in the Financial Services Industry (1st ed.) WILEY.
2. The Hong Kong Institute of Bankers (2013). Operational Risk Management (1st ed.) WILEY.
3. HKIB Handout - Fundamentals of Operational Risk Management and Risk Governance (2021)

#### **Supplementary Readings**

1. Basel Committee: Consultative Document Revisions To The Principles For The Sound Management Of Operational Risk; November 2020
2. Basel Committee: The Basel Framework: Frequently Asked Questions; June 2020
3. Basel Committee: Consultative Document Principles For Operational Resilience; August 2020
4. Basel Committee: Launch Of The Consolidated Basel Framework; December 2019
5. Basel Committee: Sound Practices: Implications Of Fintech Developments For Banks And Bank Supervisors; February 2018
6. Basel Committee: Basel III: Finalising Post-Crisis Reforms; December 2017
7. Basel Committee: Principles For The Sound Management Of Operational Risk; June 2011
8. Hong Kong Monetary Authority, TM-E-1: Risk Management of E-Banking; October 2019
9. Hong Kong Monetary Authority, IC-1: Risk Management Framework; October 2017
10. Hong Kong Monetary Authority, OR-1: Operational Risk Management in Supervisory Policy Manual; November 2005
11. Hong Kong Monetary Authority, TM-G-1: General Principles for Technology Risk Management, June 2003
12. Hong Kong Monetary Authority, TM-G-2: Business Continuity Planning, December 2002
13. Hong Kong Monetary Authority, Operational Incidents Watch
14. Hong Kong Monetary Authority, Report on Review of Self-assessments on Bank Culture; May 2020
15. Hong Kong Monetary Authority, Supervision for Bank Culture; December 2018
16. Hong Kong Monetary Authority, Bank Culture Reform; March 2017

**Further Readings**

1. McKinsey: The Future Of Operational-Risk Management In Financial Services; April 2020
2. BCG: Five Practices Of Operational Risk Leaders; October 2016
3. Accenture: The Convergence of Operational Risk and Cyber Security; 2016
4. Accenture: Reaping The Benefits Of Operational Risk Management; 2015
5. COSO Enterprise Risk Management Framework; 2021
6. ISO 31000 Risk Management Guidelines; 2018

## **Module 4: Advanced Operational Risk Management**

### **A. Module Intended Learning Outcome**

Upon completion of this module, learners should be able to:

- ✚ Develop and establish operational risk management frameworks and associated policies and procedures
- ✚ Evaluate the operational risks encountered by different business units of the AI and establish effective mitigating controls
- ✚ Manage operational risks by using risk management control tools, e.g. risk control self-assessment (RCSA) and key risk indicators (KRIs)
- ✚ Develop risk control measures by using scenario analysis and stress testing to identify potential operational risk events and assess their potential impact
- ✚ Review the risk profile of the AI/business function and apply operational risk modelling to quantify and predict operational risks
- ✚ Compile the dashboards and metrics to measure and analyse operational risks within different business units
- ✚ Develop business continuity plan and recovery strategy
- ✚ Build and promote a risk focused culture within the AI/within the business function
- ✚ Propose strategic operational risk advice and remediation actions to senior management on findings of operational risk events
- ✚ Design and deliver operational risk training to business units

### **B. Syllabus**

<b>Chapter 1: Operational Risk Assessment Methodology And New Products Risk Assessment</b>	
1	- Introduction
2	- Risk Assessment Criteria <ul style="list-style-type: none"> <li>• Optimal Risk Taking for Banks</li> <li>• Stages for Risk Assessment Process</li> <li>• Critical Risk Factors in Various Business Area</li> <li>• Operational Risk Assessment Methods</li> <li>• Operational Risk Assessment Requirements</li> <li>• Operational Risk Assessment Tools</li> <li>• Operational Risk Assessment Factors</li> <li>• Operational Risk Management Cycle</li> <li>• Timeliness of Operational Risk Assessment</li> <li>• Operational Risk Assessment Process Map</li> </ul>

3	<ul style="list-style-type: none"> <li>• Developing Assessment Criteria</li> <li>• Operational Risk Rating Scale (Sample)</li> <li>- Risk Taxonomy <ul style="list-style-type: none"> <li>• Operational Risk Taxonomy</li> <li>• Development of Operational Risk Taxonomy</li> <li>• Objective and Benefits of Operational Risk Taxonomy</li> <li>• Value of Operational Risk Taxonomy</li> <li>• Risk Taxonomy Hierarchy</li> <li>• Taxonomy by Business Lines,</li> <li>• Taxonomy by Operational Risk Event Types</li> <li>• Taxonomy by Operational Risk Causes</li> <li>• Taxonomy by Operational Risk Loss Effects</li> <li>• Taxonomy by Control Categories</li> <li>• Operational Risk Taxonomy Mapping</li> <li>• Basel Taxonomy Activity Examples (Level 3) – Loss Event Type Classification</li> <li>• Best Practice: ORX Operational Risk Taxonomy</li> <li>• Connection of the ORX Reference Taxonomy to the Basel Event Types</li> <li>• ORX Reference Taxonomy</li> <li>• ORX Bow Tie Method</li> <li>• ORX Reference Taxonomy</li> <li>• Top-level Observations From The Data</li> </ul> </li> </ul>
4	<ul style="list-style-type: none"> <li>- New Process Change Risk Assessment <ul style="list-style-type: none"> <li>• Manage Business Process Change Process</li> <li>• Types of Business Process Changes</li> <li>• Change Management R&amp;R - First Line</li> <li>• Change Management R&amp;R - Second Line</li> <li>• Business Process Change Scorecard</li> <li>• Points of Risk Consideration (Example)</li> <li>• Risk Assessment Thresholds for Business Process Change</li> <li>• Operational Risk Perspective on Change</li> <li>• Challenges on Risk Management for Changes</li> <li>• Cohorts in Responding to Change</li> <li>• Common Causes of Change Failure</li> <li>• Information Requirement on Change</li> <li>• Stage Involvement of Risk Function</li> <li>• KRI for Monitoring Project Risks</li> </ul> </li> </ul>
5	<ul style="list-style-type: none"> <li>- New Product Risk Assessment Cycle <ul style="list-style-type: none"> <li>• New Product Definition</li> </ul> </li> </ul>

	<ul style="list-style-type: none"> <li>• Industry Observation on New Product</li> <li>• Drivers for New Product</li> <li>• Features of New Product</li> <li>• Categorization of New Product</li> <li>• New Product Development Lifecycle</li> <li>• New Product Risk Assessment Requirement</li> <li>• Examples of Significant Changes to Risk Profile of Product (HKMA Illustration)</li> <li>• Principles Governing the New-Product-Approval Process</li> <li>• Issues on Managing New Product</li> <li>• Types of Risks in New Process</li> <li>• New Product Policy (Sample)</li> <li>• New Product Committee (NPC)</li> <li>• KRI for New Product</li> <li>• New Product Risk Rating (NPRR)</li> <li>• New Product Documentation</li> <li>• New Product Risk Roles and Responsibilities – First Line</li> <li>• New Product Risk Roles and Responsibilities – Second Line</li> <li>• Product Expiration</li> <li>• Consideration of Conflict of Interest</li> </ul>
6	<ul style="list-style-type: none"> <li>- Offboarding and Periodic Review <ul style="list-style-type: none"> <li>• Factors for Product Offboarding</li> <li>• Overview of Post Implementation Review</li> <li>• Scope of Post Implementation Review</li> <li>• Overview of Periodic Product Review</li> <li>• Scope of Periodic Product Review</li> </ul> </li> </ul>
7	<ul style="list-style-type: none"> <li>- Case Studies <ul style="list-style-type: none"> <li>• Case Study: Mis-selling of Investment Products</li> <li>• Case Study: Deficient practices in ascertaining insurance protection for bill discounting business</li> <li>• Case Study: Underpayment of stamp duty for certain OTC transactions</li> </ul> </li> </ul>
8	<ul style="list-style-type: none"> <li>- Best Practice Guidance <ul style="list-style-type: none"> <li>• New Product Checklist (Sample)</li> </ul> </li> </ul>
<b>Chapter 2: Scenario Analysis And Stress Testing</b>	
1	<ul style="list-style-type: none"> <li>- Introduction</li> </ul>
2	<ul style="list-style-type: none"> <li>- Stress Testing <ul style="list-style-type: none"> <li>• Definition of Scenario Analysis, Stress Testing and Reverse Stress Testing</li> <li>• Relationship between Scenario Analysis, Stress Testing and Reverse Stress Testing</li> </ul> </li> </ul>

	<ul style="list-style-type: none"> <li>• Demarcating Scenario Analysis, Stress and Reverse Stress testing</li> <li>• Overview and Risk Factors of Operational Risk Stress Testing</li> <li>• Value of Operational Risk Stress Testing</li> <li>• Elements of Operational Risk Stress Testing</li> <li>• Types of Risks Covered in Stress Testing</li> <li>• Guiding Principles of Stress Testing</li> <li>• Purpose of Stress Testing and Scenario Analysis</li> <li>• Features of Stress Testing and Scenario Analysis</li> <li>• Benefits of Stress Testing and Scenario Analysis</li> <li>• Linkage to Capital Planning Process</li> </ul>
3	<ul style="list-style-type: none"> <li>- Scenario Analysis           <ul style="list-style-type: none"> <li>• Overview of Scenario Analysis</li> <li>• Conducting Effective Scenario Analysis</li> <li>• Identifying and Agreeing the Focus of Analysis</li> <li>• Determining the Level of Analysis</li> <li>• Key Components of Scenario Analysis Framework</li> <li>• Scenario Design and Scenario Execution</li> <li>• Approach in Developing Scenario Analysis</li> <li>• Governance and Responsibilities</li> </ul> </li> </ul>
4	<ul style="list-style-type: none"> <li>- Selection of The Scenarios           <ul style="list-style-type: none"> <li>• Animal Kingdom of Risks</li> <li>• Black Swam Examples</li> <li>• Gray Rhino Examples</li> <li>• Questions on Understanding the Unknowns</li> <li>• Steps in Building Scenario Analysis</li> <li>• Relevance of Scenario Analysis</li> <li>• Forward-looking Focus</li> <li>• Data Collection</li> <li>• Scenario Risk Drivers</li> <li>• Scenario Distribution</li> <li>• High Severity Scenario Examples</li> <li>• Scenario Biases</li> <li>• Possible Relationships between Operational Losses and Macroeconomic Conditions for Basel Event Types</li> <li>• Identifying and Approving a Portfolio of Scenarios</li> <li>• Techniques for Identifying Scenarios</li> <li>• Sample of Common Scenarios (Corporate Bank)</li> <li>• Assessing COVID Impact with Scenario Analysis</li> </ul> </li> </ul>



5	- Execution and Analysis <ul style="list-style-type: none"> <li>• Running a Scenario Workshop</li> <li>• Causes of Scenarios</li> <li>• Assessing Impacts</li> <li>• Assessing Likelihood</li> <li>• Management Response</li> <li>• Scenario Template</li> <li>• Expert Assessment and Biases</li> <li>• Validation and Governance</li> <li>• Preparing for Operational Risk Workshop</li> <li>• Conducting a Workshop</li> <li>• The Participants</li> <li>• Assessing Probability and Impact</li> <li>• Workshop Analysis Techniques</li> <li>• Validation of Output</li> <li>• Governing the Process</li> <li>• Making Effective Use of the Outputs</li> <li>• Risk and Capital Modeling</li> <li>• Calculating Baseline Loss</li> <li>• Expected Levels of Loss</li> <li>• Unexpected Levels of Loss</li> <li>• Key Challenges in Scenario Analysis</li> </ul>
6	- Benchmarking with The Industry <ul style="list-style-type: none"> <li>• Industry Benchmarking of Scenario Analysis</li> <li>• Industry Survey on Scenario Analysis</li> </ul>
7	- Regulatory Guideline <ul style="list-style-type: none"> <li>• Global Regulatory Timeline</li> <li>• BCBS Principles for Sound Stress Testing Practices and Supervision</li> <li>• HKMA Requirement on Stress Testing and Operational Risk Scenario Analysis</li> </ul>
8	- Case Studies <ul style="list-style-type: none"> <li>• Case Study: Phishing emails and fraudulent bank websites stealing customers' e-banking account information</li> </ul>
9	- Best Practice Guidance <ul style="list-style-type: none"> <li>• Stress Testing Toolkit</li> <li>• Reverse Stress Testing Methodology</li> </ul>
<b>Chapter 3: Key Risk Indicators</b>	
1	- Introduction
2	- Difference Between Key Risk Indicator, Key Control Indicator and Key Performance

3	<p>Indicator</p> <ul style="list-style-type: none"> <li>• Definitions of Operational Risk Indicators</li> <li>• Risk Indicators</li> <li>• Control Indicators</li> <li>• Performance Indicators</li> <li>• Dimensions and Types of Key Risk Indicators</li> <li>• KRI vs KCI vs KPI</li> <li>• Composite Indicators</li> <li>• Essentials of Key Indicators</li> <li>• Categories of Key Risk Indicators</li> <li>• Exposure Indicators</li> <li>• Failure Indicators</li> <li>• Stress Indicators</li> <li>• Causal Indicators</li> <li>• BCBS Principles</li> </ul> <p>- Design</p> <ul style="list-style-type: none"> <li>• Life Cycle of Key Risk Indicators</li> <li>• Roles of Key Risk Indicators</li> <li>• Translating Risk Appetite</li> <li>• Risk Monitoring</li> <li>• Governance and Assurance</li> <li>• Risk Assessment and Modelling</li> <li>• Relevance</li> <li>• Measurable</li> <li>• Leading vs Lagging Indicators</li> <li>• Types of Indicators</li> <li>• Bow Tie Diagram for Key Risk Indicators</li> <li>• Easy to Collect and Monitor</li> <li>• Comparable</li> <li>• Auditable</li> <li>• Selecting Indicators: Top Down or Bottom Up</li> <li>• Consideration for Top-down Approach</li> <li>• Consideration for Bottom-up Approach</li> <li>• Deciding Frequency</li> <li>• Consideration for Number of Key Risk Indicators</li> <li>• Thresholds and Limits</li> <li>• Specialized Thresholds</li> <li>• Value Proposition of Risk Indicators</li> </ul>
---	--

4	- Analysis	<ul style="list-style-type: none"> <li>• Analysis of Loss Related Indicators</li> <li>• Analysis of Cause Related Indicators</li> <li>• Analysis of Control Related Indicators</li> <li>• Risk Monitoring</li> <li>• Triggers for Escalation</li> <li>• Managing and Reporting Risk Indicators</li> <li>• Adding or Changing Indicators</li> <li>• Taking Action to Resolve Threshold or Limit Breaches</li> <li>• Comparative Analysis – Joining the Dots</li> <li>• Overview of KRI Reporting</li> </ul>
5	- Reporting	<ul style="list-style-type: none"> <li>• Level of KRI Reporting</li> <li>• Reporting to Different Audiences</li> <li>• Frequency of Reporting</li> <li>• Data Visualisation</li> </ul>
6	- Validation	<ul style="list-style-type: none"> <li>• Validating Indicators</li> <li>• Governance, Responsibilities and Assurance</li> </ul>
7	- Case Studies	<ul style="list-style-type: none"> <li>• Case Studies: The Monetary Authority Suspends CHUI Chau Mang For Four Months</li> <li>• Case Studies: Enforcement Collaboration - Pang Hon Pan Banned For 21 Months</li> </ul>
8	- Best Practice Guidance	<ul style="list-style-type: none"> <li>• Sample Key Risk Indicators (KRI)</li> <li>• Sample Key Performance Indicators (KPI)</li> <li>• Sample Key Control Indicators (KCI)</li> <li>• Sample KRI Reports</li> <li>• Success Factors in Op Risk Reporting</li> </ul>
<b>Chapter 4: Capital Requirements For Operational Risk</b>		
1	- Introduction	
2	- Basic Indicator Approach (BIA)	<ul style="list-style-type: none"> <li>• Operational Risk Capital Calculation</li> <li>• Capital Approach</li> <li>• BCBS Principles</li> <li>• Position of Various Capital Measurement Approach</li> <li>• Selection Criteria</li> </ul>

3	<ul style="list-style-type: none"> <li>• Basic Indicator Approach</li> <li>• BIA Example 1</li> <li>• BIA Example 2</li> </ul> <p>- Standardized Approach (SA)</p> <ul style="list-style-type: none"> <li>• The Standardized Approach</li> <li>• Advantages of Standardized Approach</li> <li>• TSA Example 1</li> <li>• TSA Example 2</li> </ul>
4	<p>- Alternative Standardized Approach (ASA)</p> <ul style="list-style-type: none"> <li>• Alternative Standardized Approach</li> </ul>
5	<p>- Advanced Measurement Approach (AMA)</p> <ul style="list-style-type: none"> <li>• Advanced Measurement Approach</li> <li>• Advanced Measurement Approach Distribution Curve</li> <li>• AMA Quantitative Stipulations</li> <li>• AMA Qualitative Stipulations</li> <li>• Internal Measurement Approach</li> <li>• Loss Distribution Approach</li> <li>• Advantages and Disadvantages of LDA</li> <li>• Standard LDA methods</li> <li>• Step 1: Modeling Frequency</li> <li>• Frequency in an LDA Model: Example</li> <li>• Qualities of the Poisson Distribution</li> <li>• Step 2: Modeling Severity</li> <li>• Selecting a Severity Distribution</li> <li>• The Severity Probability Distribution</li> <li>• Step 3: Monte Carlo Simulation</li> <li>• Correlation</li> <li>• Scenario Analysis Approach to Modeling Operational Risk Capital</li> <li>• Advantages and Disadvantages of an SA Approach</li> <li>• Hybrid Approach to Modeling Operational Risk Capital</li> <li>• Insurance</li> <li>• Disclosure</li> </ul>
6	<p>- Revised Standardized Approach (RSA)</p> <ul style="list-style-type: none"> <li>• Revised Standardized Approach</li> <li>• Methodology of Revised Standardized Approach</li> <li>• Reduced Risk Management Incentive</li> <li>• Implications For Banks (Data, systems and processes, business model, capital)</li> <li>• Business Indicator Component</li> </ul>

7	-	<ul style="list-style-type: none"> <li>• Loss Component</li> </ul>
8	-	<ul style="list-style-type: none"> <li>• Case Studies</li> <li>• Case Study: Insufficient controls over storage of title deeds of customers</li> </ul>
	-	<ul style="list-style-type: none"> <li>• Best Practice Guidance</li> <li>• Data Comparability Problem</li> <li>• Changing Level of Operational Risk Capital</li> <li>• Operational Risk Management Road Map</li> <li>• Operational Risk Allocation Rules</li> <li>• Charging Framework (Sample)</li> </ul>
<b>Chapter 5: Risk Control Self-Assessment</b>		
1	-	Introduction
2	-	<ul style="list-style-type: none"> <li>Operational Risk Process and Key Control Analysis</li> <li>• Definition of RCSA</li> <li>• Types and Approaches of RCSA</li> <li>• General Control Environment Self-Assessment on Minimum Expected Controls</li> <li>• Characteristics of RCSA</li> <li>• Benefits of RCSA</li> <li>• Key Business Identification</li> <li>• Governance and Responsibilities</li> <li>• Frequency and Timing</li> <li>• BCBS Principles</li> </ul>
3	-	<ul style="list-style-type: none"> <li>Process Risk Mapping and Control</li> <li>• Business Process and Process Risk</li> <li>• Sign off on the Business Process</li> <li>• Tools on Operational Risk Mapping</li> <li>• Key Operational Risk Process by Function</li> </ul>
4	-	<ul style="list-style-type: none"> <li>Business Process Management Tool</li> <li>• Business Process Management</li> <li>• Root Cause Analysis</li> <li>• Operational Risk Event Types</li> <li>• Operational Risk Causal Factors</li> <li>• Risk Assessment Criteria</li> <li>• Subjective Risk Assessment</li> <li>• RCSA – Scorecard Approach</li> <li>• RCSA – Questionnaire Approach</li> <li>• RCSA Proactive Risk Identification and Management Tool</li> <li>• Management Results Reporting Tools</li> <li>• Heat Mapping</li> </ul>

5	<ul style="list-style-type: none"> <li>• Operational Frequency – Severity Risk Mapping</li> <li>• RCSA Follow Up</li> <li>• Advantage and Disadvantage of RCSA</li> </ul>
6	<ul style="list-style-type: none"> <li>- Quantification of Potential Exposure           <ul style="list-style-type: none"> <li>• Risk (Probability and Impact) Matrix</li> <li>• Quantification Techniques</li> <li>• Maximum Potential Exposure</li> </ul> </li> </ul>
6	<ul style="list-style-type: none"> <li>- Residual Risk Assessment and Treatment           <ul style="list-style-type: none"> <li>• Inherent Risk Exposure</li> <li>• Residual Risk Exposure</li> <li>• Causes</li> <li>• Effects</li> <li>• Action Plan</li> <li>• Other Elements</li> <li>• Risk Treatment Strategies</li> <li>• Operational Risk Action Plan</li> </ul> </li> </ul>
7	<ul style="list-style-type: none"> <li>- Operational Risk Reporting and Dashboards           <ul style="list-style-type: none"> <li>• Reporting RCSA Results</li> <li>• Reporting Action Planning</li> <li>• Internal Audit Planning and Reporting</li> </ul> </li> </ul>
8	<ul style="list-style-type: none"> <li>- Case Studies           <ul style="list-style-type: none"> <li>• Case Study: Misappropriation of a customer's funds by a staff member using a returned ATM card</li> </ul> </li> </ul>
9	<ul style="list-style-type: none"> <li>- Best Practice Guidance           <ul style="list-style-type: none"> <li>• Top-Down and Bottom-Up</li> <li>• Completing an RCSA: Approaches and Techniques</li> <li>• Workshop Approach</li> <li>• Planning</li> <li>• Attendees</li> <li>• Structure and Duration of the Workshop</li> <li>• Facilitation</li> <li>• Validation</li> <li>• Questionnaires</li> <li>• Scope of Questionnaire</li> <li>• Designing a Questionnaire</li> <li>• Content of Questionnaire</li> <li>• Integrating an RCSA into the Operational Risk Management Framework</li> </ul> </li> </ul>
<b>Chapter 6: Operational Risk Events</b>	

1	-	Introduction
2	-	Different Types of Risk Events <ul style="list-style-type: none"> <li>• Definition of Operational Risk Event</li> <li>• Identification of Loss Events</li> <li>• Brainstorming Loss Events</li> <li>• Defining Loss Events</li> <li>• Screening Loss Events</li> <li>• Factors of Review of Loss Events</li> <li>• Actual Events and Near Misses</li> <li>• Categorisation of Events</li> <li>• Governance and Responsibilities</li> <li>• BCBS Principles</li> </ul>
3	-	Root Cause Analysis <ul style="list-style-type: none"> <li>• Root Cause Analysis</li> <li>• Fault Tree Analysis</li> <li>• Ishikawa Cause and Effect Diagram</li> <li>• Causes of Risk Events</li> <li>• Control Failures</li> <li>• Direct And Indirect Impacts</li> <li>• Financial and Non-Financial Impacts</li> <li>• Aligning with the Wider Operational Risk Framework</li> <li>• Operational Risk Causal Factors</li> <li>• Operational Risk Effect Types</li> </ul>
4	-	Data Collection <ul style="list-style-type: none"> <li>• Data Capture Requirements</li> <li>• Reasons of Data Collection</li> <li>• Date and Time of the Event</li> <li>• Risk Event Type</li> <li>• Location</li> <li>• Causes</li> <li>• Control Failures</li> <li>• Direct and Indirect Impacts</li> <li>• Financial and Non-Financial Impacts</li> <li>• External Data Collection</li> <li>• Data Collection: Difficulties and Solutions</li> <li>• Aligning with the Wider Operational Risk Framework</li> </ul>
5	-	Escalation <ul style="list-style-type: none"> <li>• Incident Management and Notification</li> </ul>

	<ul style="list-style-type: none"> <li>• Loss Prediction</li> <li>• Loss Prevention</li> <li>• Loss Control</li> <li>• Loss Reduction</li> <li>• Assumptions, Avoidance and Transference</li> <li>• Reporting of Operational Risk Events</li> <li>• Using Operational Risk Event Data</li> <li>• Using Loss Data to Support Risk Assessments and Monitoring</li> <li>• Using Loss Data to Support The Risk Appetite and Tolerance Activities</li> <li>• Using External Data to Benchmark Internal Loss Data</li> <li>• Using Loss Data to Support the Identification of Emerging Risks</li> <li>• Insight and Oversight</li> <li>• Supporting Risk Governance</li> </ul>
6	<ul style="list-style-type: none"> <li>- Treatment of Boundary Loss <ul style="list-style-type: none"> <li>• Treatment of Credit Risk Related Operational Risk Events</li> <li>• Treatment of Market Risk Related Operational Risk Events</li> <li>• Goodwill Payment</li> <li>• Single Versus Many Events</li> <li>• Specific Criteria on Loss Data Identification, Collection and Treatment</li> <li>• General Criteria on Loss Data Identification, Collection and Treatment</li> <li>• Lesson Learnt Session</li> </ul> </li> </ul>
7	<ul style="list-style-type: none"> <li>- Lesson Learnt and Corrective Actions <ul style="list-style-type: none"> <li>• Source Data Documentation</li> <li>• Training and Awareness</li> <li>• Review on Other ORM Tools</li> <li>• External Event Analysis</li> </ul> </li> </ul>
8	<ul style="list-style-type: none"> <li>- Case Studies <ul style="list-style-type: none"> <li>• Case Study: Misappropriation of a customer's funds by a staff member using a returned ATM card</li> </ul> </li> </ul>
9	<ul style="list-style-type: none"> <li>- Best Practice Guidance <ul style="list-style-type: none"> <li>• Thematic reviews</li> <li>• Risk Modelling</li> <li>• Risk Culture</li> <li>• Reasons for collecting Operational Risk Event/Loss Data</li> <li>• Connecting multiple, related events</li> <li>• Validation of loss estimates</li> <li>• When to close an event</li> </ul> </li> </ul>

### Chapter 7: Regulatory And Supervisory Frameworks



1	-	Introduction
2	-	Compliance with Regulatory Standards <ul style="list-style-type: none"> <li>Recap on Hong Kong Monetary Authority, SA-1: Risk Management Framework; October 2017</li> <li>Recap on Hong Kong Monetary Authority, OR-1: Operational Risk Management; November 2005</li> </ul>
3	-	Supervisory Approach of Regulators <ul style="list-style-type: none"> <li>HKMA Risk-based Supervisory Approach</li> <li>Relationship with the Prudential Regulator</li> <li>Continuous Supervision</li> <li>The HKMA's Risk-based Supervisory Methodology</li> <li>Risk Assessment Exercise</li> <li>Consolidated Supervision</li> <li>HKMA Risk Assessment on AI</li> <li>Primary prudential obligations of an AI</li> </ul>
4	-	On-Site Examination and Prudential Meetings <ul style="list-style-type: none"> <li>Preparation for On-site Examinations</li> <li>Preparation for Off-site Reviews</li> <li>Prudential Meetings</li> </ul>
5	-	Guidelines from The BCBS (10) <ul style="list-style-type: none"> <li>Recap on Basel Committee: Principles For The Sound Management Of Operational Risk; June 2011</li> <li>Recap on Basel Committee: Revisions to the principles for the sound management of operational risk: August 2020</li> <li>Basel Committee: Consolidated Basel Framework April 2019</li> </ul>
6	-	Regulatory Focus <ul style="list-style-type: none"> <li>HKMA 2020 Focus</li> <li>HKMA 2021 Work Priorities</li> </ul>
7	-	Case Studies <ul style="list-style-type: none"> <li>Case Study: Account takeover using a lost HKID card</li> </ul>
8	-	Best Practice Guidance <ul style="list-style-type: none"> <li>Regulatory Compliance Toolkit</li> </ul>
<b>Chapter 8: Contingency, Business Continuity And Recovery Planning</b>		
1	-	Introduction
2	-	Types of Resilience Risk <ul style="list-style-type: none"> <li>Definition of Resiliency</li> <li>Threats to Financial Resilience</li> <li>Interconnects of Financial and Operational Resiliency</li> </ul>

3	-	<ul style="list-style-type: none"> <li>• Drivers of Operational Resilience</li> <li>• Risk, Resilience and Sustainability</li> </ul>
4	-	<ul style="list-style-type: none"> <li>• Resiliency Risk Framework</li> <li>• Operational Resilience Framework</li> <li>• Questions on Operational Resilience</li> <li>• Common Challenges</li> <li>• COVID-19 Challenges</li> <li>• Building Blocks of Operational Resilience</li> <li>• Approach to Operational Resiliency</li> </ul>
5	-	<ul style="list-style-type: none"> <li>• Effective Tools of Planning, Execution and Testing</li> <li>• Business Continuity Planning</li> <li>• Business Continuity Execution</li> <li>• Business Continuity Testing and Review</li> <li>• Business Continuity Insurance</li> </ul>
6	-	<ul style="list-style-type: none"> <li>• Regulatory Requirements</li> <li>• Overview of International Regulation and Standard</li> <li>• Evolution of Regulation on Operational Resiliency (UK)</li> <li>• Meeting Regulator Expectation</li> <li>• Regulators Step Up Pressure</li> <li>• Resilience is a Governance Issue</li> <li>• IOSCO Principles on Cyber-resilience</li> <li>• BCBS Consultation on Operational Resiliency August 2020</li> <li>• HK Regulator Position on COVID-19</li> </ul>
7	-	<ul style="list-style-type: none"> <li>• Integration into Operational Risk</li> <li>• Enterprise Resiliency Office</li> <li>• Maintaining Financial Resiliency In Post COVID-19</li> <li>• Integration Operational Resiliency into Operational Risk</li> </ul>
8	-	<ul style="list-style-type: none"> <li>• Case Studies</li> <li>• Case Study: Guide to Better Operational Resilience</li> </ul>
9	-	<ul style="list-style-type: none"> <li>• Best Practice Guidance</li> <li>• Take-away on Resiliency Risk Management</li> <li>• BCP Checklist</li> </ul>
<b>Chapter 9: Risk Culture, Awareness And Key Components Of Successful Operational Risk Management Implementation</b>		
1	-	<ul style="list-style-type: none"> <li>• Introduction</li> </ul>
2	-	<ul style="list-style-type: none"> <li>• Risk Culture and Awareness</li> <li>• Recap on the Importance of Operational Risk Culture</li> <li>• Performance Metrics of Operational Risk Culture</li> </ul>

3	<ul style="list-style-type: none"> <li>- Importance and Application of Trainings in Operational Risk Management           <ul style="list-style-type: none"> <li>• Operational Risk Training</li> <li>• Means of Operational Risk Training</li> <li>• Contents of Operational Risk Training</li> <li>• Review and Maintain Operational Risk Training</li> </ul> </li> </ul>
4	<ul style="list-style-type: none"> <li>- Communication and Engagement Plan of Operational Risk Management in The Workplace           <ul style="list-style-type: none"> <li>• Motive: Reduce Routine Losses and Improve Efficiency</li> <li>• Motive: Reduce the Required Amount of Regulatory Capital</li> <li>• Motive: Improve Operational Efficiency</li> <li>• Motive: Overcome Operational Risk Challenges</li> <li>• Methods of Communication and Engagement</li> </ul> </li> </ul>
5	<ul style="list-style-type: none"> <li>- Communication with Senior Management on Operational Risk Topics           <ul style="list-style-type: none"> <li>• Communication on Elements of Operational Risk Framework</li> <li>• Communication on Risk Can Be Aggregated and Presented in Simple and Concise Manner to Senior Management</li> <li>• Communication on Interpretation of High Level Operational Risk Results to Draw</li> <li>• Communication on Meaningful Conclusions and Trends That Will Impact the Organization</li> <li>• Communication on Explanation of Operational Risk Measurement Tools and Methodologies in Simple and Concise Manner to All Business Units and Senior Management</li> <li>• Operational Risk Reporting Process</li> <li>• Common Content of ORM Reports</li> <li>• Successful Factors in ORM Reporting and Why They Are Important</li> <li>• Risk Report Best Practice Examples</li> <li>• What Does This Mean In Practice</li> <li>• Objectives of Operational Risk Reporting</li> <li>• Characteristics of Operational Risk Reporting</li> <li>• Contents in Operational Risk Reports (Examples)</li> <li>• Operational Risk Reports</li> </ul> </li> </ul>
6	<ul style="list-style-type: none"> <li>- Oversight, Monitoring and Understanding of Relevant Operational Risk Management Processes Taken Up by Subject Matter Experts           <ul style="list-style-type: none"> <li>• Engagement Model between Operational Risk and Internal Audit</li> <li>• Engagement Model between Operational Risk and Compliance</li> <li>• Engagement Model between Operational Risk and Business Continuity</li> </ul> </li> </ul>

7	<ul style="list-style-type: none"> <li>• Engagement Model between Operational Risk and Other Subject Matter Experts</li> </ul>
	- Case Studies
8	<ul style="list-style-type: none"> <li>• Case Study: Enforcement action against Société Générale by the SFC following the investigation of the HKMA</li> </ul>
	- Best Practice Guidance
	<ul style="list-style-type: none"> <li>• ORM Implementation Toolkit</li> </ul>

### Chapter 10: Operational Risks Related To The Key Areas For Future Banking

1	- Introduction
2	- Green and Sustainable Banking
	<ul style="list-style-type: none"> <li>• Current Landscape</li> <li>• Climate Risk Concept</li> <li>• Types of Climate Risks</li> <li>• Climate Risk Impact</li> <li>• Physical and Transition Risk</li> <li>• Key Climate Related Risk for Financial Institutions</li> <li>• Managing Climate Risk</li> <li>• Climate Risk and Opportunities</li> <li>• Task Force on Climate Related Financial Disclosure (TCFD)</li> <li>• TCFD Recommendations</li> <li>• TCFD Supplement Guidance</li> <li>• How Banks Addressing Climate Risk</li> <li>• TCFD Key Implementation Challenges</li> <li>• Typology of Physical Risk</li> <li>• From Physical Risk to Financial Stability Risk</li> <li>• Typology of Transition Risk</li> <li>• From Transition Risk to Financial Stability Risk</li> <li>• Climate Financial Risk Assessment</li> <li>• Example of Climate Risk Impact on Bank</li> <li>• How Financial Firms Addressing Climate Risk</li> <li>• Climate Risk Framework</li> <li>• Four Biodiversity-related Financial Risks</li> <li>• Operational Risk Assessment</li> <li>• Climate Risk Stress Testing</li> <li>• Operational Risk Scenarios (Example)</li> <li>• Incorporating Climate Risk into Enterprise Risk</li> </ul>
3	- Digital Banking Services
	<ul style="list-style-type: none"> <li>• Journey of Intelligent Process Automation</li> </ul>

	<ul style="list-style-type: none"> <li>• Adversarial Risk</li> <li>• Risk Assessment Framework</li> <li>• Technology Risk Assessment Framework</li> <li>• Third Party Risk Assessment Framework</li> <li>• Recognition of Risk and Control</li> <li>• Proactive Risk and Control Consciousness</li> <li>• Call to Action</li> <li>• Emerging Risk in Fintech</li> <li>• Risk Questions to Answer</li> <li>• Operational Risk in Retail Payments and Digital Wallets</li> <li>• Operational Risk in Fintech Credit</li> <li>• Operational Risk in Robo-advisors</li> <li>• Operational Risk in DLT-based Wholesale Payment Systems</li> <li>• Operational Risk in Private Digital Currencies</li> <li>• Operational Risk in AI and Machine Learning</li> </ul>
4	- Case Studies <ul style="list-style-type: none"> <li>• Case Study: The HKMA suspends Leung Wai Yu for three months</li> </ul>
5	- Best Practice Guidance <ul style="list-style-type: none"> <li>• Risk Management for New Initiatives Toolkit</li> </ul>
<b>Chapter 11: The Future and Challenges Of Operational Risk Management</b>	
1	- Introduction
2	- Competence Development <ul style="list-style-type: none"> <li>• ORM Officer Professional Standard Summary of Core Competencies</li> <li>• HK SFC Managers-In-Charge of Core Functions (MIC)</li> <li>• HKMA Enhanced Competence Framework for Banking Practitioners</li> <li>• Strengthening Individual Accountability</li> </ul>
3	- Emerging and Proactive Risk Management <ul style="list-style-type: none"> <li>• Performing Environmental Scanning</li> <li>• Proactive ORM Monitoring</li> <li>• Forces Driving Complexity, Increasing Risk</li> <li>• Identification of Emerging Risks and Opportunities</li> <li>• Use of Operational Risk in Decision Making</li> <li>• Early Warning Signal</li> <li>• Develop Scenarios</li> <li>• Generate Options and Strategy</li> <li>• Implement Strategy</li> <li>• Review Risk Development</li> <li>• Effective Lines of Defense</li> </ul>

4	-	<ul style="list-style-type: none"> <li>• Predictive Risk Intelligence</li> <li>• Embedding Operational Risk into Business</li> <li>• Overview of Deliverables by Stakeholders</li> </ul> <p>Deployment of Artificial Intelligence</p> <ul style="list-style-type: none"> <li>• Key Trends in Risktech</li> <li>• Application of Technology in the Financial and Non-financial Risk Management</li> <li>• Priority of RegTech and RiskTech</li> <li>• GARP Survey on AI/RPA</li> <li>• AI Adoption in Risk Management</li> <li>• Risk Managers in Assessing AI Adoption or Non-adoption Risk</li> <li>• Empower Risk and Compliance</li> <li>• Trade Lifecycle Enabled by AI</li> <li>• Digitization of Risk Management</li> <li>• CCAR and Stress Testing</li> <li>• Risks and Opportunities: Questions on AI</li> <li>• Risks on AI</li> <li>• Key Points on AI Development Path</li> </ul>
5	-	<p>Challenges and Solutions</p> <ul style="list-style-type: none"> <li>• Integrating ORM Framework</li> <li>• Engaging the Right People</li> <li>• Adding Value</li> <li>• Overcoming the Cultural Challenges</li> <li>• What Does Success Look Like</li> <li>• Key Elements to Embed Operational Risk</li> <li>• Operational Risk Deliverables</li> </ul>
6	-	<p>Case Studies</p> <ul style="list-style-type: none"> <li>• Case Study: The Monetary Authority Suspends Chu Lai Kwan for Breaching the Code of Conduct and Internal Policy of Her Employer</li> </ul>
7	-	<p>Best Practice Guidance</p> <ul style="list-style-type: none"> <li>• Overcome ORM Challenges Toolkit</li> </ul>
<b>Chapter 12: Integrated Case Studies And Best Practices</b>		
1	-	Introduction
2	-	<p>Integrated Case Studies</p> <ul style="list-style-type: none"> <li>• Operational Risk Lessons from the OCC's Citibank Fine</li> <li>• Swiss banks suffer tax-dodging fines</li> <li>• Aussie banks pay for underpaying staff</li> </ul>
3	-	<p>Best Practice Guidance</p> <ul style="list-style-type: none"> <li>• Interbank payment weaknesses</li> </ul>

- |  |   |
|--|---|
|  | <ul style="list-style-type: none"> <li>• Swiss tax evasion</li> <li>• Data breaches top \$2bn since 2012</li> </ul> |
|--|---|

### **C. Recommended Readings**

#### **Essential Readings:**

1. Ariane Chappelle (2018). Operational Risk Management: Best Practices in the Financial Services Industry (1st ed.) WILEY.
2. The Hong Kong Institute of Bankers (2013). Operational Risk Management (1st ed.) WILEY.
3. HKIB Handouts - Advanced Operational Risk Management (2021)

#### **Supplementary Readings:**

1. Basel Committee: Consultative Document Revisions To The Principles For The Sound Management Of Operational Risk; November 2020
2. Basel Committee: The Basel Framework: Frequently Asked Questions; June 2020
3. Basel Committee: Consultative Document Principles For Operational Resilience; August 2020
4. Basel Committee: Launch Of The Consolidated Basel Framework; December 2019
5. Basel Committee: Sound Practices: Implications Of Fintech Developments For Banks And Bank Supervisors; February 2018
6. Basel Committee: Basel III: Finalising Post-Crisis Reforms; December 2017
7. Basel Committee: Principles For The Sound Management Of Operational Risk; June 2011
8. Hong Kong Monetary Authority, TM-E-1: Risk Management of E-Banking; October 2019
9. Hong Kong Monetary Authority, IC-1: Risk Management Framework; October 2017
10. Hong Kong Monetary Authority, OR-1: Operational Risk Management in Supervisory Policy Manual; November 2005
11. Hong Kong Monetary Authority, TM-G-1: General Principles for Technology Risk Management, June 2003
12. Hong Kong Monetary Authority, TM-G-2: Business Continuity Planning, December 2002
13. Hong Kong Monetary Authority, Operational Incidents Watch
14. Hong Kong Monetary Authority, Report on Review of Self-assessments on Bank Culture; May 2020
15. Hong Kong Monetary Authority, Supervision for Bank Culture; December 2018
16. Hong Kong Monetary Authority, Bank Culture Reform; March 2017

#### **Further Readings:**

1. McKinsey: The Future Of Operational-Risk Management In Financial Services; April 2020
2. BCG: Five Practices Of Operational Risk Leaders; October 2016
3. Accenture: The Convergence of Operational Risk and Cyber Security; 2016
4. Accenture: Reaping The Benefits Of Operational Risk Management; 2015
5. COSO Enterprise Risk Management Framework; 2021
6. ISO 31000 Risk Management Guidelines; 2018

## 7. Training Application

### A. Training Schedule

For the latest information about the training application period and class schedules, please contact HKIB staff or refer to HKIB website at <https://www.hkib.org/page/87>.

### B. Training Duration

The training durations of Core Level and Professional Level are set out as follows:

Training Mode	Lecture
Training Duration*	Module 1 – 15 Hours Module 2 – 15 Hours Module 3 – 15 Hours Module 4 – 21 Hours

*\*The stated training duration are set as the standard training duration for the whole programme. If you have any special request and situation for a different training duration, please contact HKIB staff for special arrangement.*

### C. Training Application

Applicants can obtain an application form: (i) from HKIB website; or (ii) in person from the counter of HKIB Head Office during office hours

Application Requirements:

- ✚ The information provided for the training enrolment must be true and clear.
- ✚ For enrolment, applicants can return the application form via email, by hand, by registered mail (to avoid loss in transit) or submit via the electronic application form in HKIB webpage. Attention should be paid to the application deadline. Postal applicants are reminded to allow sufficient time for mailing or a late entry fee will be charged.
- ✚ Inaccurate or incomplete applications may not be accepted even if the applicant has paid the training fee.
- ✚ Each applicant should submit only ONE application form for each programme.
- ✚ HKIB reserves the right to reject late applications and/or any applications deemed inappropriate. Once HKIB has received an application form, NO alterations to the training arrangement are allowed.



- ✚ HKIB reserves the right to change training dates and application deadlines at any time.
- ✚ Applicants are advised to retain a copy of the completed application form for their own records.

#### D. Training Fee and Payment

Module	Training Duration	Training Fee
1	15 Hours	HKD3,750*
2	15 Hours	HKD3,750*
3	15 Hours	HKD3,750 <sup>#</sup>
4	21 Hours	HKD6,060 <sup>#</sup>

\* For Module 1 & Module 2, a digital version of training material (i.e. Study Guide and PPT Slides) will be provided before the training commencement. Printed version will only be available at an additional cost of HKD500 (including delivery fee) on request by learners.

# For Module 3 & Module 4, only a digital version of PPT Slides will be provided before the training commencement. Printed version will only be available at an additional cost of HKD500 (including delivery fee) on request by learners. In addition, learners have to purchase two reference books by their own as a part of the essential readings.

- ✚ Applicants should pay the training fee as follows:
  - (a) By cheque (post-dated cheques are not accepted), attached to the application form. Cheques/E-cheques should be made payable to "The Hong Kong Institute of Bankers"; **OR**
  - (b) By credit card. Please provide your credit card information on the application form.
- ✚ Application forms without payment instructions are **NOT** processed.
- ✚ All payments must be settled before the start of the programme. **NO** fees are refunded or transferred under any circumstances.
- ✚ Applicants are advised to keep a record of their payment.
- ✚ Confirmation of training application is sent to applicants via email at least **5 working days** prior to the training date.

- ✚ Late training enrolment will be accepted after the stipulated application deadline up to seven days before course commencement to allow us to administer the application. A late entry fee of HKD200 (in addition to the training fee) will apply.
- ✚ HKIB reserves the right to adjust training application, study guide and/or administration surcharge fees (if applicable), at any time.

## 8. Examination Application and Regulations

### A. Examination Mode and Format

The examination mode and format for Core Level are as follows:

<b>Module</b>	1 - 2	3
<b>Examination Mode</b>	Paper-based Examination	
<b>Examination Duration</b>	1.5 Hours per Module	2.5 Hours per Module
<b>Question Type</b>	Multiple-choice Type Questions (MCQs)	
<b>No. of Questions</b>	50-60 MCQs per Module	80-90 MCQs per Module
<b>Pass Mark</b>	70%	
<b>Grading</b>	Grade	Mark Range
	Pass with Distinction	Above 90%
	Pass with Credit	80% - 90%
	Pass	70% - 79%
	Fail A	60% - 69%
	Fail B	50% - 59%
	Fail C	Below 50%
	Absent	N/A

The examination mode and format for Professional Level are as follows:

<b>Module</b>	4	
<b>Examination Mode</b>	Paper-based Examination	
<b>Examination Duration</b>	3 Hours	
<b>Question Type</b>	Multiple-choice Type Questions (MCQs) & Essay Type Questions	
<b>No. of Questions</b>	40-50 MCQs with 2-3 essay type questions	
<b>Pass Mark</b>	60%	
<b>Grading</b>	Grade	Mark Range
	Pass with Distinction	Above 85%
	Pass with Credit	75% - 85%
	Pass	60% - 74%
	Fail A	56% - 59%
	Fail B	46% - 55%
	Fail C	Below 46%
	Absent	N/A

## **B. Examination Timetable**

- ✚ For latest information about the examination application period and examination dates, please contact HKIB staff or refer to HKIB website at <https://www.hkib.org/page/87>.

## **C. Examination Application**

- ✚ Candidates taking current training classes can choose to sit for the current examination or any subsequent ones. They can choose to sit for subsequent examinations but if the corresponding programme has been changed or updated, they may be required to re-take the training in order to be eligible for module examination.
- ✚ Applicants can obtain an application form: (i) from HKIB website; or (ii) in person from the counter of HKIB Head Office during office hours.
- ✚ For enrolment, applicants can return the application form via email, by hand, by registered mail (to avoid loss in transit) or submit via the electronic application form in HKIB webpage. Attention should be paid to the application deadline. Postal applicants are reminded to allow sufficient time for mailing or a late entry fee will be charged.
- ✚ The information provided on the application form must be true and clear. Applicants should submit a completed and signed application form, together with the appropriate examination fee, to HKIB Head Office on or before the corresponding application deadline.
- ✚ Late examination enrolment will be accepted after the stipulated application deadline up to 14 days before examination date, to allow us to administer the application. A late entry fee of HKD 200 (in addition to the examination fee) will apply.
- ✚ Inaccurate or incomplete applications may not be accepted even if the applicant has paid the examination fee.
- ✚ Each applicant should submit only ONE application form for each examination.
- ✚ Under no circumstances are changes to module entry allowed.
- ✚ HKIB reserves the right to reject late applications and/or any applications deemed inappropriate. Once HKIB has received the application form, NO alterations to the examinations and examination arrangements are allowed.
- ✚ HKIB reserves the right to change examination dates and application deadlines at any time.

- Applicants are advised to retain a copy of the completed application form for their own records.

#### **D. Examination Fee and Payment**

	<b>Module 1 / 2</b>	<b>Module 3</b>	<b>Module 4</b>
<b>First attempt</b>	HKD 530	HKD 1,060	HKD 1,300
<b>Re-attempt</b>	HKD 530	HKD 1,060	HKD 1,300

- Applicants should pay the examination fee:
  - By cheque (post-dated cheques are not accepted), attached to the application form. Cheques/E-cheques should be made payable to "The Hong Kong Institute of Bankers"; OR
  - By credit card. Please provide your credit card information on the application form.
- Application forms without payment instruction are NOT processed.
- All payments must be settled before the examination. NO fees are refunded or transferred under any circumstances.
- Applicants are advised to keep a record of their payments.
- Acknowledgement of the examination application is sent to candidates via email within seven working days of receipt of application form. Candidates who fail to receive an acknowledgement within this time should inform the Institute immediately.
- HKIB reserves the right to adjust the examination, study guide and/or administration surcharge fees (if applicable), at any time.

#### **E. Examination Attendance Notice**

- Examination Attendance Notices (Attendance Notices) are sent to candidates via email ONLY approximately two weeks before the examination. Candidates must inform the Institute if they have not received it one week before the examination.
- Candidates are required to print a copy of the Attendance Notice on a sheet of plain A4 paper before attending each examination.
- Candidates MUST present their Attendance Notice at the examination along with a valid identification document (e.g. an HK Identity Card or passport) bearing a current photograph. Photocopies are not accepted.

**F. Alteration/Transfer of Application for an Examination**

- ✚ HKIB reserves the right to cancel, postpone and/or reschedule the examination.
- ✚ If an examination is rescheduled, HKIB notifies candidates of the new date and time via email within 1 week of the original schedule. Under such circumstances, candidates are not required to re-register for the examination.
- ✚ Under no circumstances are any changes to or transfers of examination application allowed.

**G. Examination Arrangements for Candidates with Special Needs**

- ✚ Candidates with special needs may request special examination arrangements. Under these circumstances they are required to submit documentary evidence, such as medical proof issued by a registered medical practitioner, together with a written request, when applying for the examination. Approval of the request is subject to final HKIB decision.
- ✚ Request for such arrangements may result in an additional charge.

**H. Examination Preparation**

- ✚ Candidates enrolled in the examination are required to study all the essential, recommended and further reading material, if applicable, as part of their examination preparation.

## **I. Examination Results**

- ✚ For Core Level examination, candidates receive a result slip by post two to four weeks from the examination date. For Professional Level examination, candidates receive a result slip by post six to eight weeks from the examination date.
- ✚ Results are not revealed by telephone, fax or email.
- ✚ Candidates may check their examination results online through HKIB online platform. Candidates receive email notification once the examination results are available. The online examination results are removed one month after they are released.
- ✚ Results are withheld from candidates who have not paid in full any monies due or payable to the Institute, including but not limited to examination application fees.
- ✚ Candidates may request rechecking or remarking of their examination scripts (not applicable to MCQ examinations) within one month of the issue of examination results by submitting a written request. An administrative fee may apply. Please contact HKIB staff for details.

## J. General Examination Regulations

An examination is governed by the regulations in force at the time of the examination and not at the time of application, in case there are discrepancies between the two sets of regulations.

On all matters concerning interpretation of the regulations, the Professional Standard and Examination Board of the Institute has the final decision.

- ✚ Candidates must complete the training class before taking the examination.
- ✚ The examination is conducted in English.
- ✚ Candidates must use an HB/2B pencil to answer the multiple-choice questions on the Answer Sheets.
- ✚ Examinations are conducted and invigilated by responsible persons appointed by HKIB.
- ✚ Examination Attendance Notices are sent to candidates via email **ONLY**. Candidates are required to print a copy on a plain sheet of A4 paper and **MUST** take their Attendance Notice to each examination, along with a valid identification document (e.g. HK Identity Card or passport). Attendance Notices are collected by the invigilators before the end of the examination, if necessary.
- ✚ Candidates should arrive at the examination venue at least 15 minutes before the start. Candidates must not enter the examination room until instructed to do so.
- ✚ Candidates are not allowed to sit for the examination if they are unable to present Attendance Notice/valid identification document, or if the identification document does not contain a clear and current photograph of the candidate.
- ✚ All examinations begin at the time stated on the Attendance Notice. Latecomers may be admitted during the first 30 minutes of the examination, but extra time will not be given to compensate for any time lost



- ✚ Smoking, eating and drinking are not allowed in the examination room. All mobile phones and other electronic devices must be switched off.
- ✚ All bags, books and other personal belongings must be placed in a location advised by the invigilator, before the examination begins.
- ✚ If you need to go to the toilet during the examination, you should seek permission from an invigilator. An invigilator will accompany you and you must NOT carry any mobile phones, other electronic devices, question books, answer sheets or other papers to the toilet.
- ✚ No other aids, such as books, dictionaries, computers (e.g. notebooks, PC tablets) or papers are permitted in the examination. No draft paper is provided during the examination. Rough workings or notes should be made on the question book and will not be marked.
- ✚ The packets of question papers are opened in the presence of the candidates before the start of the examination. Candidates should remain silent and are not allowed to communicate with other candidate during the examination. Candidates interfering with the proper conduct of the examinations are warned by the invigilator or expelled from the examination room in a serious case. Under such circumstances, a report is submitted to HKIB to consider whether disciplinary action should be taken. Disciplinary action includes, but is not limited to, candidate disqualification.
- ✚ Candidates cannot leave the examination room during the first 45 minutes and the last 15 minutes of an examination. Candidates who decide to leave early must notify the invigilator as quietly as possible, and are not allowed to re-enter the examination room.
- ✚ Candidates must stop writing when instructed to do so by the invigilator.
- ✚ Candidates must not detach any part of their answer sheet, or remove their answer sheet, wholly or partly, from the examination room.
- ✚ Candidates are not allowed to communicate with other candidates during an examination. They are also prohibited from communicating with third parties outside the examination room by using any electronic device. The invigilator has the right to expel candidates from the examination room if their behaviour interferes with the proper conduct of the examination. Any candidate attempting to copy from another candidate's script or any other source is disqualified.

- ✚ Pocket calculators: Financial calculators may be used and listed below

#### Calculator Model

- Texas Instruments: BA II Plus (both versions), including the BA II Plus Professional
- Hewlett Packard: HP 10B, HP 10bII, HP 10bII+, HP12C (including the HP 12C Platinum and the Anniversary Edition), HP 12C Prestige, HP 17bII+, HP20B
- Sharp: Sharp Business/Financial Calculator EL-733, EL-733a
- Casio: FC 100/FC 100V/FC 200/FC 200V

*Newer and older versions of these calculators will be allowed into the examination room*

HKIB strictly enforces all policies with regard to calculator usage during examinations and candidates are required to abide by the policies of HKIB. Calculators are inspected prior to the start of the exam. They must remain on your desk in full view and proctors continue to inspect calculators throughout the administration of the examination. Possession or use of an unauthorised calculator at the test centre results in the voiding of your examination results and may lead to the suspension or termination of your candidacy in HKIB Programme. Failure by the proctors to detect an unauthorised calculator prior to the start of the examination, or your use of an unauthorised calculator at any time during the examination, does not imply that the calculator is an approved model or that your scores will ultimately be reported. Calculator covers, keystroke cards, and loose batteries are permitted in the testing room; instruction manuals are not.

- ✚ Candidates are required to clear financial calculator memory prior to each session of the examination. (Please do not ask invigilators to clear it.) It is candidates' responsibility to revert their own calculator to desired setting(s) once the calculator's memory has been cleared. If a candidate's calculator has notes/formulas printed on the back of the calculator, includes pull-out cards or contains other supplemental material, this information must be removed or masked by solid colour tape before entering the examination room.
- ✚ If any candidate infringes any of the above regulations, he/she is liable to disciplinary actions, including disqualification.

## 9. Certification Application and Renewal Process

### A. Certification Application

Relevant Practitioners who have completed Modules 1 to 3 of the “ECF on Operational Risk Management (ORM) (Core Level)” programme and obtained a pass in the relevant examinations, may apply for AORP Certification with HKIB professional membership.

Relevant Practitioners who have completed Modules 4 of the “ECF on Operational Risk Management (ORM) (Professional Level)” programme and obtained a pass in the relevant examination, may apply for CORP Certification with HKIB professional membership.

Relevant Practitioners are required to submit a completed Certification Application Form for AORP/ CORP to HKIB together with the relevant supporting documents and payment of the required Certification Fee. The Certification Application Form can be obtained from [HKIB website](#) or HKIB Head Office.

AORP/ CORP holders are registered as Certified Individuals and included in the public register on HKIB website. Upon successful application for AORP/ CORP Certification with HKIB, HKIB also grants the AORP/ CORP holders a HKIB professional membership.

### B. Certification Renewal

The AORP and CORP certification is subject to annual renewal by HKIB.

AORP and CORP holders are required to comply with the annual Continuing Professional Development (CPD) Scheme in order to renew their Certification. The requirement is a minimum of 12 verifiable CPD hours, at least six of which must be earned from activities related to the topics of compliance, legal and regulatory requirements, risk management and ethics. The remaining hours should be related to banking and finance or the job function.

AORP and CORP holders are to renew their certification registration annually in January. Debit notes are issued prior to the renewal deadline. Certification holders who do not pay the continuing membership subscription on or **before 31 January of each calendar year** are treated as Default Members.

### C. Certification Fee and Payment



The application fee for Certification in various categories are as follows:  
(Valid until 31 December 2022)

<b>Certification</b>	1 <sup>st</sup> year certification - Non-HKIB member: HKD1,650 - HKIB ordinary member: HKD570 - HKIB professional member: <b>Waived</b> - HKIB senior member: HKD1,450
<b>Certification Renewal</b>	Annual Renewal - Certification: HKD1,650 - Re-registration fee of default member: HKD2,000



Applicants should pay the Certification Fee and Certification Renewal Fee:

- Paid by Employer
- By cheque (post-dated cheques are not accepted), attached to the application form. Cheques/E-cheques should be made payable to "The Hong Kong Institute of Bankers"; **OR**
- By credit card. Please provide your credit card information on the application form.



Application forms without payment instruction are **NOT** processed.



**NO** fees are refunded or transferred under any circumstances.



Applicants are advised to keep a record of their payment.



HKIB reserves the right to adjust the certification, re-certification and/or administration surcharge fees (if applicable), at any time.

### D. Certification and HKIB Membership Regulations

It is mandatory for all individuals to maintain a valid membership status with HKIB if the applicants want to apply for and maintain AORP/ CORP certification and be subject to HKIB membership governance.

Once an application is processed, the membership subscription and registration fees are non-refundable and non-transferable.

The name of the member to be entered on HKIB's records is that on the certification application form. This name, and the order and spelling in which it is presented are used subsequently on all transcripts, pass lists, diplomas, and certificates except where a member has notified HKIB of any change. Such notification must be accompanied by a certified true copy<sup>1</sup> of documentary confirmation, e.g. Hong Kong Identity Card, birth certificate, statutory declaration, etc.

AORP/ CORP holders are bound by the prevailing rules and regulations of HKIB. They are to abide by HKIB's rules and regulations in HKIB [Members' Handbook](#). AORP/ CORP holders are required to notify HKIB of any material changes to responses to any of the questions in certification application, including their contact details. HKIB may investigate the statements AORP/ CORP holders make with respect to applications, and they may be subject to disciplinary actions for any misrepresentation (whether fraudulent and otherwise) in their applications.

AORP/ CORP holders have the responsibility to notify HKIB of any material changes to responses to personal information required, including contact details. HKIB may investigate the statements the applicant makes with respect to certification application, and that the applicant may be subject to disciplinary actions for any misrepresentation (whether fraudulent and otherwise) in certification application.

### ***E. Membership Reinstatement***

Members who have not paid the annual subscription fees when due shall be considered as default members, and are not entitled to use any HKIB Professional Qualification, and nor may call themselves members of the Institute.

Default members who reinstate their membership with HKIB are required to pay the current year's subscription plus a Re-registration fee. Once the memberships reinstated, the member's examination record, if any, is reactivated.

---

<sup>1</sup> Submitted copies of documents to HKIB must be certified as true copies of the originals by:

- HKIB designated staff; or
- HR/authorized staff of current employer (Authorized Institution); or
- A recognized certified public accountant / lawyer / banker / notary public; or
- Hong Kong Institute of Chartered Secretaries (HKICS) member.

- Certifier must **sign** and **date** the copy document (printing his/her **name** clearly in capitals underneath) and clearly indicate his/her **position** on it. Certifier must state that it is a true copy of the original (or words to similar effect)

## 10. Exemption Application and Regulations

### 10.1 Module Exemption Requirements

The following arrangements are made for candidate to obtain exemption for modules of the “Advanced Certificate of ECF on Operational Risk Management (ORM)”.

Module	Eligibility for exemption
Module 1	RP who has passed the following related training programmes <ul style="list-style-type: none"> <li>• Certification in Risk Management Assurance of the Institute of Internal Auditors; or</li> <li>• Bachelor’s or higher degree in law; or</li> <li>• Professional Ethics and Compliance module under the Advanced Diploma for Certified Banker (Stage I) of the HKIB; or</li> <li>• Certified Professional Risk Manager of the Asia Risk Management Institute (ARIMI); or</li> <li>• Certified Public Accountant of the Hong Kong Institute of Certified Public Accountants (HKICPA);</li> <li>• Full member of Association of Chartered Certified Accountants (ACCA); or</li> <li>• Members of overseas accountancy bodies which are eligible for full exemption from the qualification programme for membership admission at the HKICPA under the HKICPA’s reciprocal membership and mutual recognition agreements (as listed on its website)</li> </ul>
Module 3	RP who has passed the following related training programmes <ul style="list-style-type: none"> <li>• Operational Risk Manager Certificate of the Professional Risk Managers’ International Association (PRMIA); or</li> <li>• Professional Risk Manager of the PRMIA; or</li> <li>• Certificate in Operational Risk Management of the Institute of Operational Risk (IOR), which is now a part of the Institute of Risk Management (IRM) group.</li> </ul>

## 10.2 Module Exemption Application

- ✚ Candidate with relevant qualifications may apply for module exemption from “Advanced Certificate for ECF on Operational Risk Management (ORM)”.
- ✚ Exemption application should be made on an exemption form together with the following documents/items; failing to do so may delay the assessment:
  - i. Appropriate fees (application fee and exemption fees)
  - ii. Copies of transcript and certificate, if applicable
- ✚ Documents submitted are not returned regardless of the application result.
- ✚ Unless otherwise specified, exemption application based on partially attained qualification is not accepted.
- ✚ Exemption claims granted to student members are only registered in HKIB’s record upon the student members’ graduation.
- ✚ Exemption results are normally given in writing within two months after receipt of application and supporting documents. If further assessment is needed due to unexpected circumstances, separate notifications are given. The decision of the Institute is final and cannot be appealed.
- ✚ Candidate attempting but failing in a module may subsequently claim exemption from that module if they obtain a new/further qualification recognised for exemption purposes.
- ✚ An exemption confirmation letter is issued to candidate whose exemption application is granted.
- ✚ Candidate exempted from a module subsequently attempting that module by examination, have their exemption status overridden.

## 11. General Information

### 11.1 Bad Weather Arrangements

In the event of bad weather on the training class/examination day, candidates should visit HKIB website at [www.hkib.org](http://www.hkib.org) for announcements about the latest arrangements, and should pay attention to radio/television broadcasts about weather conditions.

- If the typhoon signal No. 8 or above, black rainstorm signal, or “extreme conditions” is hoisted or still in force on the day of a training class, the arrangements below apply:

Signal in force	Training Class(es) cancelled
At 6:30am	Morning Session (8:30am – 2:00pm) is cancelled.
At 12:00noon	Afternoon Session (2:00pm – 6:00pm) is cancelled.
At 3:00pm	Evening Session (6:00pm – 10:00 pm) is cancelled.

- If the typhoon signal No. 8 or above, black rainstorm signal, or “extreme conditions” is hoisted or still in force on the day of an examination at the following times, the arrangements below will apply:

Signal in force	Examination cancelled
At 6:00am	Examination(s) (8:00am – 1:00pm) are cancelled.
At 10:00am	Examination(s) (1:00pm – 5:00pm) are cancelled.
At 2:00pm	Examination(s) (at 5:00pm or after) are cancelled.

- If typhoon signal No. 8 or above, black rainstorm signal, or “extreme conditions” is hoisted or still in force while the training class/examination is in progress, the training class/examination continues as scheduled.
- If a training class/examination is rescheduled, HKIB notifies candidates of the new training class/examination date and time by email within **one week** of the originally scheduled date. Under such circumstances, candidates are not required to re-register for the training class/examination. Applications for a refund and/or transfer are NOT allowed.



- ✚ HKIB reserves the right to postpone, cancel and/or reschedule any training class/examination.

### **12.2 Personal Data Protection Policy**

Personal data provided by the candidate are used for administrative and communicative purposes relating to training and examination. Failure to provide complete and accurate information may affect the provision of administrative services to the candidate. The Institute keeps the personal data provided confidential, but may need to disclose it to appropriate personnel in the Institute and other relevant parties engaging in the provision of examination services to the Institute. Candidates have the right to request access to and correction of their personal data. For details, candidates can contact the Institute.

Candidates are advised to read the Personal Data Protection Policy at **Appendix** to understand their rights and obligations in respect of the supply of personal data to HKIB and the ways in which HKIB may handle such data.

### **12.3 Addendums and Changes**

HKIB reserves the right to make changes and additions to membership, training and examination regulations, enrolment/application procedures, information in this handbook and any related policies without prior notice. HKIB shall bear no responsibility for any loss to candidates caused by any change or addition made to the aforementioned items.

## 12. Contact information

### HKIB Head Office Address

3/F Guangdong Investment Tower, 148 Connaught Road Central, Hong Kong



### General Enquiries

Tel.: (852) 2153 7800 Email: [cs@hkib.org](mailto:cs@hkib.org)

### Training and Programme Enquiries

Tel.: (852) 2153 7800 Email: [ecf@hkib.org](mailto:ecf@hkib.org)

### Membership Enquiries

Tel.: (852) 2153 7879 Email: [membership@hkib.org](mailto:membership@hkib.org)

### Examination Enquiries

Tel.: (852) 2153 7821 Email: [exam@hkib.org](mailto:exam@hkib.org)

### Certification Enquiries

Tel.: (852) 2153 7865 Email: [cert.gf@hkib.org](mailto:cert.gf@hkib.org)

### Office Service Hours

Monday – Friday: 09:00 - 18:00