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)

* 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 31/07/2030)

\# 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 31/07/2030)

Table of Contents

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.

Since the implementation of ECF in 2018, various programmes for different job functions in banking industry have been developed and integrated into The Hong Kong Institute of Bankers' (HKIB) flagship Certified Banker (CB) Programme which offer generalist, specialist, and strategic topics. The rationale for putting all programmes under one professional banking qualification is to promote an industry-based common qualifications benchmark. While ECF programmes offer "role-based" knowledge and certification to relevant practitioners, CB is offering a vocational qualification pathway for further career advancement, being continuously enhanced to nurture more holistic banking professionals and ultimately, supporting the industry to develop a continuous learning culture and a sustainable talent pool so as to maintain the competitiveness of Hong Kong as an international financial centre.

The Enhanced Competency Framework on Operational Risk Management (ECF-ORM) was introduced to develop a sustainable pool of operational risk management practitioners for the banking industry. The qualification structure of the ECF-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-ORM, HKIB has developed the learning programme – the **"ECF on Operational Risk Management (Core Level)"** to help individuals attain the Core Level of the competency standards set for the ECF-ORM. The programme **"ECF on Operational Risk Management (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-ORM 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 Guide to Enhanced Competency Framework on Operational Risk Management dated 18 December 2020 issued by HKMA or you may visit HKIB ECF on Operational Risk Management webpage.

2. Background

2.1 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 thebanking industry; and

(ii) To raise the professional competence of operational risk management practitioners in thebanking industry.

2.2 Competency Standards

They are set at two levels:

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 5 or less years of experience.

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

2.3 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 anAI 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 is 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 – ECF-ORM: Key roles and tasks for Relevant Practitioners of the HKMA the Guide to Enhanced Competency Framework on Operational Risk Management.

2.4 Certification and Public Register

There are two Professional Qualifications under the ECF-ORM:

Core Level

Associate Operational Risk Management Professional (AORP)

A Relevant Practitioner may apply to HKIB for the 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; or

(2) is grandfathered based on the required work experience upon the launch of the Core Level module and employed by an AI at the time of application.

** *Module 1 and Module 2 are identical for both ECF on Operational Risk Management and ECF on Compliance. Hence, an RP who has completed Module 1 and/or Module 2 under either of these ECF streams will not be required to complete the same module(s) under the other ECF stream.*

Professional Level

Certified Operational Risk Management Professional (CORP)

A Relevant Practitioner may apply to HKIB for professional certification if he or she:

(1) has completed Module 4 of the Professional Level training programme and obtained a pass in the relevant examination module on top of the Core Level qualification plus at least five years

(should be accumulated within the ten years immediately prior to the date of application for certification, but need not to be continuous) of relevant experience as specified in "Annex 1 stated in HKMA's "Guide to Enhanced Competency Framework on Operational Risk Management"; or

(2) is grandfathered based on the required work experience upon the launch of the Professional Level module and employed by an AI at the time of application.

For details regarding grandfathering requirements, please refer to HKIB website and section 7 of the HKMA the Guide to Enhanced Competency Framework on Operational Risk Management .

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

Learners who have successfully completed a HKIB professional qualification programme (including training and examination requirements) but yet to fulfil the requirement of Relevant Practitioners or required years of relevant work experience for certification will be automatically granted as ECF Affiliate.

ECF Affiliate holders are then registered as Certified Individuals and included in the public register on HKIB website. Ordinary Membership with membership fee for the awarding year waived will also be granted to learners.

2.5 Annual renewal of certification and CPD Requirements

The ECF-ORM certification is subject to annual renewal by HKIB. PQ holders are required to meet the annual Continuing Professional Development (CPD) requirements and pay an annual certification renewal 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), of which at least 6 CPD hours should be on topics related to 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.

For ECF Affiliate, at least 3-hours of CPD within the scopes mentioned in HKIB CPD Scheme is required annually for certification renewal.

No CPD is required in the first year when the above certification(s) is granted. The CPD requirement starts in the following calendar year.

Please refer to the Overview of HKIB CPD Scheme and HKIB CPD Requirements webpage for more details.

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 thestipulated minimum entry requirements:

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

Remarks:

1. *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.*

3.2 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.

3.3 Programme Intended 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; and
- Analyse operational risk metrics and use operational risk reporting and dashboards to identify the potential operational risks.

3.4 Learning Hours

The programme design adopts a blended learning approach. Learners are advised to spend not less than 400 Learning Hours (equivalent to 40 credits) in total for completing a full Programme. 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.

The Programme comprise of the following 3 modules as accumulated a total of 40 credits:
Module 1: Ethics and Corporate Governance in Banking Industry (10 credits)
Module 2: Regulatory Framework and Compliance in Banking Industry (10 credits)
Module 3: Fundamentals of Operational Risk Management and Risk Governance (20 credits)

3.5 Completion Requirements

The completion period for the Programme is eight years from the year in which the first module is completed.

Learners are required to complete all three modules and accumulated a total of 40 credits by obtaining a pass in all relevant examinations.

3.6 Integration in Certified Banker (CB)

The "ECF on Operational Risk Management (Core Level)" is integrated in the Certified Banker (Stage I) as one of the Elective Modules.

CB (Stage I) is a professional banking qualification programme developed and offered by HKIB. It is intended to raise the professional competency of banking and financial practitioners in Hong Kong to meet modern demands, while providing a transparent standard with international recognition.

Individuals who have completed the "ECF on Operational Risk Management (Core Level)"

programme and obtained a pass at the relevant examination or have been grandfathered "Advanced Certificate for ECF on Operational Risk Management (Core Level)" programme and obtain a pass at HKIB's exemption assessment are encouraged to join the CB (Stage I) Programme.

3.7 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 31/07/2030).

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 Outcomes

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

- Develop and establish operational risk management frameworks and associated policies and procedure;
- 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; and
- Design and deliver operational risk training to business units.

4.4 Learning Hours

The programme design adopts a blended learning approach. Learners are advised to spend not less than 300 Learning Hours (equivalent to 30 credits) for completing the following module. 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.

Module 4: Advanced Operational Risk Management (30 credits)

4.5 Integration in Certified Banker (CB)

The "ECF on Operational Risk Management (Professional Level)" is integrated in the Certified Banker (Stage II) as one of the Elective Modules.

CB (Stage II) is a professional banking qualification programme developed and offered by HKIB. It is intended to raise the professional competency of banking and financial practitioners in Hong Kong to meet modern demands, while providing a transparent standard with international recognition.

Individuals who have completed the "ECF on Operational Risk Management (Professional Level)" programme and obtained a pass at the relevant examination or have been grandfathered "Professional Certificate for ECF on Operational Risk Management (ORM)" programme and obtain a pass at HKIB's exemption assessment are encouraged to join the CB (Stage II) Programme.

4.6 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 31/07/2030)

Please refer to the accreditation page on HKIB website for more details.

5. Learning Support

HKIB provides learners with a range of support services to help you throughout the learning journey. These services include answering your enquiries, managing the certification process, providing access to library resources, offering study materials, and maintaining an online learning platform. The aim of these services is to facilitate learners and increase the chances of success in the training and examination. Here are some highlights for your attention.

5.1 Video-On-Demand

To facilitate the learners to get better preparation for the examination, HKIB provides the Video-On-Demand service for the learners to watch the recorded training sessions of a particular training class. Video-On-Demand service is available for up to 90 days before the examination.

5.2 Professional Qualification Programme Scholarship Scheme

Each year, HKIB selects the top two candidates from each competency level (Core/Professional) and award them with the scholarship as recognition. This is the way for HKIB to promote academic excellence and motivate future students to push themselves to achieve same high level of performance.

The two top candidates in each competency level (Core/Professional), provided that all other granting requirements are met, can be awarded with a cash incentive (HKD4,000 for Core Level; HKD5,000 for Professional Level), and a study coupon which can provide candidates to study one more professional qualification offered by HKIB with all training and examination fees waived.

5.3 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 Cornerfor borrowing. To provide updated learning resources to the members, HKIB has provided FREEinternet 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.

5.4 Market Information Updates

HKIB regularly organises training courses, CPD programmes, conference, seminars and luncheon talks, industry events on current issues and developments in financial markets that learners may find essential, helpful and relevant to their learning. Besides, HKIB provides members with updated market information through complimentary bi-monthly journal Banking Today, weekly e-news and first-hand internship opportunities.

For more details, please refer to Events & Industry Initiatives and HKIB eLearning under HKIB website.

5.5 Mock Examination Paper for Examination Preparation

To facilitate the learners to get better preparation for the examination, HKIB provides the mock examination paper for the learners as reference to better understand the examination format, structure and approach. Thus, all the questions shared from the mock examination paper will NOT be used in the official examination.

5.6 Learning Consultation Services

For learners require any learning consultation services related to the banking professional qualifications offered by HKIB, they may contact us through our customer service hotline at (852) 2153 7800 for making arrangement.

6. Programme Syllabus

6.1. Module 1: Ethics and Corporate Governance in Banking Industry

(As mentioned in 2.4, this Module is identical to ECF on Compliance Module 1.)

A. Module Objective

This module aims to provide the candidates with essential knowledge related to major areas of professional ethics, risk and compliance in the context of corporate governance. The respective ethical and compliance aspects and issues encountered by individuals or corporations in the second line of defence in the context of the boarder risk environment is to be explained.

B. Module Intended Outcomes

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 effectivecompliance;
- Identify different roles associated in building a culture for effective management of governance, risk, and compliance in financial institution; and
- Apply regulatory requirement and effective compliance control on daily duties by demonstrating an understanding of and adopting the requirement related to corporate governance;

C. Syllabus

Chapter 1: Business Ethics	
1.1	**Definition of Compliance and Operational Risk and the linkage with Ethics and Law**
1.2	**Overview of Business Ethics**
1.2.1	- What is Business Ethics
1.2.2	- The importance of Business Ethics
1.2.3	- Approaches to Normative Ethics: Absolutism and Relativism
1.3	**Ethics and the Individual**
1.3.1	- Code of Conduct
1.3.2	- Understanding Ethical Decision-making Process
Chapter 2: Ethics and the Corporation	
2.1	**Introduction: Corporate social responsibility, Corporate accountability and Corporate citizenship**
2.2	**Corporate Social Responsibility**
2.2.1	- International Consensus
2.2.2	- The pros and cons of implementing corporate social responsibility
2.2.3	- The impact of Globalisation
2.3	**Social Environmental Issues Facing Banks**
2.3.1	- Environmental, Social Responsibility, Governance (“ESG”)
2.3.2	- Equator Principles on Project Financing
2.3.3	- Case study: “The Sustainability Report: The role of Bank on Sustainability”
2.3.4	- Local ESG authorities
2.3.5	- Green financing
2.4	**Understanding Reputational Risk**
2.4.1	- Key drivers of Reputation
2.4.2	- Public Perception and Reputation Risk
2.4.3	- Case studies: The Bank Runs
Chapter 3: Risk Management: Principles and Concepts	
3.1	**Introduction: The importance of risk management as the key to effective compliance**
3.2	**Definition of Risk**
3.2.1	- Definition of Risk
3.2.2	- Different types of Risk in Banking (HKMA approach)
3.2.3	- Other approaches to categorise risk
3.3	**The Basic of Risk Management Framework**
3.3.1	- Enterprise Risk Management Framework – the Three Lines of Defence
3.3.2	- Key Elements of Effective Risk Management (ISO 31000: 2018 Risk Management Guideline)
3.3.3	- The Three Lines of Defence (SPM IC-1 and Basel Requirement)

3.3.4	- Organisational structure for an effective Risk Management Framework
3.4	**An Overview of Key Risk Management Process**
3.4.1	- Risk Identification
3.4.2	- Risk Measurement, Risk Analysis and Evaluation
3.4.3	- Risk monitoring and reporting
3.4.4	- Risk mitigation
3.4.5	- Methodologies and Governance of an Effective Risk Management Framework
Chapter 4: The Regulators, Law and Regulation	
4.1	**Introduction: The Prudential Approach**
4.2	**Key Functions of Financial Regulators**
4.2.1	- The Hong Kong Monetary Authority ("HKMA")
4.2.2	- The Securities and futures Commission ("SFC")
4.2.3	- The Insurance Authority ("IA")
4.2.4	- The Mandatory Provident Fund Schemes Authority ("MPFSA")
4.3	**Regulatory Requirements**
4.3.1	- An Overview
4.3.2	- Know Your Customers / Due Diligence
4.3.3	- Suitability Obligations and Mis-selling
4.3.4	- Market misconduct under the Securities and Futures Ordinance
4.3.5	- Protecting the Customers
Chapter 5: Corporate Governance in Banks	
5.1	**Introduction**
5.1.1	- What is Corporate Governance
5.1.2	- Corporate Governance Principles for Banks (Basel Committee)
5.2	**Agency Theory**
5.2.1	- Agency theory
5.2.2	- Agency costs
5.2.3	- The public interest in financial stability
5.2.4	- The misalignment between the interests of bank shareholders and the public interest
5.2.5	- Case Study: Libor Manipulation and subsequent ethical ramification: the emergence of SOFR
5.3	**The Role and Composition of the Board**
5.3.1	- Structure of banks
5.3.2	- Stakeholders in Corporate Governance
5.3.3	- Regulatory Requirement and Implication
5.4	**Accountability of Banks**
5.4.1	- Introduction
5.4.2	- Disclosure
5.4.3	- Transparency
Chapter 6: Remuneration and Appointment of Board Members, Chief Executive and Managers	
6.1	**Introduction: The Competence of Board Directors and Chief Executive in Banks**
6.2	**Principal Forms of Directorial and Executive Remuneration**
6.2.1	- Basic Director's service fee
6.2.2	- Executive salary
6.2.3	- Bonus payments
6.2.4	- Shares and restricted share grants
6.2.5	- Executive share options
6.3	**Determination of Remuneration**
6.3.1	- Fundamental principles: the guideline from Hong Kong Institute of Directors
6.3.2	- The function of Remuneration committee
6.3.3	- Determination of Non-executive Directors' remuneration
6.3.4	- Guideline on a sound remuneration system (CG-5)
6.4	**Appointments of Chief Executives and Directors**
6.4.1	- Section 71 of Banking Ordinance

6.4.2	- HKMA Requirements (CG-1, s. 6, 7)
6.5	**Appointments of Bank Managers**
6.5.1	- Section 72B of Banking Ordinance
6.5.2	- HKMA Requirements (CG-2, s. 3)
Chapter 7: Internal Control and Compliance in Banking	
7.1	**Introduction: A Risk Based Approach to Bank Supervision (World Bank Paper Chp.15)**
7.2	**The Elements of Internal Control System**
7.2.1	- Elements of Internal Control System
7.2.2	- Attributes of an effective control system
7.2.3	- The Three Lines of Defence
7.3	**Costs and Benefits of Internal Control**
7.3.1	- Costs
7.3.2	- Benefits
7.3,3	- Case Study: Manipulation of US GSE debt securities trading before 2008
7.3.4	- Case Study: The integrity of the financial system
7.4	**Second Line of Defence: The Compliance Function**
7.4.1	- Regulatory Requirement (IC-1)
7.4.2	- The Compliance functions
7.4.3	- The role of Compliance Officer
7.5	**The Role of Risk Management Function to Effective Control and Compliance in Banks**
7.5.1	- The Voluntary Boundary
7.5.2	- Core practice
7.5.3	- Mandated boundary
7.5.4	- Case Study: An example from Data Quality Management

D. Recommended Readings

Essential Readings:

1. HKIB Study Guide of ECF-ORM: Module 1 Ethics and Corporate Governance in Banking Industry. (2025).

Supplementary Readings

1. Iris H.-Y. Chiu. (2015). The Law of Corporate Governance in Banks. Edward Elgar Publishing.

Further Readings

1. John R. Boatright. (2014). Ethics in Finance (3rd ed.). Wiley-Blackwell.
2. Joël Bessis. (2015). Risk Management in Banking (4th ed.). John Wiley & Sons, Ltd.
3. Hong Kong Monetary Authority. Website and Supervisory Policy Manual.
4. Securities and Futures Commission. (2024). Code of Conduct for Persons Licensed by or Registered with the Securities and Futures Commission.
5. ISO 31000: 2018 Risk management Guidelines

6.2. Module 2: Regulatory Framework and Compliance in Banking Industry

(As mentioned in 2.4, this Module is identical to ECF on Compliance Module 2.)

A. Module Objective

This module aims to provide candidates with both a board overview of the regulatory framework governing banks in Hong Kong and in depth understanding and application of compliance requirements applicable to banks in Hong Kong covering the various regulatory regimes under the following regulators and governing laws.

B. 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 specificallythe 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, aswell 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 basedon the legal and regulatory requirement, develop strategies to mitigate the risks maintaining compliance position of the bank at the tolerance level; and
- 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.

C. Syllabus

Chapter 1: Overview of Regulatory Regime for Bank in Hong Kong	
1.1	**Overall Financial Regulatory Framework in Hong Kong**
1.1.1	- Overview of the Financial Market in Hong Kong
1.1.2	- Major Types of Business in the Financial Market
1.1.3	- Why Financial Markets Must Be Regulated
1.1.4	- The Basic Regulatory Model of the Financial Business
1.1.5	- Financial Regulation
1.1.6	- Different Financial Regulators in Hong Kong
1.2	**Hong Kong Monetary Authority – Regulatory Framework**
1.2.1	- Definition of Banking Business
1.2.2	- Banking Ordinance and its Subsidiary Legislation
1.2.3	- Different Types of Authorised Institution
1.2.4	- HKMA - History and Background
1.2.5	- HKMA - Regulatory Powers

1.2.6	- HKMA - Role and Composition
1.2.7	- HKMA - Relationship with Banks
1.3	**Securities and Futures Commission – Regulatory Framework**
1.3.1	- Definition of Securities-related Business
1.3.2	- Securities and Futures Ordinance and its Subsidiary Legislation
1.3.3	- Licensed Corporation vs Registered Institution
1.3.4	- SFC - History and Background
1.3.5	- SFC - Regulatory Powers
1.3.6	- SFC - Role and Composition
1.3.7	- SFC - Relationship with Banks
1.4	**Insurance Authority – Regulatory Framework**
1.4.1	- Definition of Insurance Business
1.4.2	- Insurance Ordinance and its Subsidiary Legislation
1.4.3	- Different Types of Insurance Business
1.4.4	- IA - History and Background
1.4.5	- IA - Regulatory Powers
1.4.6	- IA - Role and Composition
1.4.7	- IA - Relationship with Industrial Bodies
1.4.8	- IA - Relationship with Banks
1.5	**Mandatory Provident Fund Scheme Authority – Regulatory Framework**
1.5.1	- Definition of MPF Business
1.5.2	- Mandatory Provident Fund Schemes Ordinance and its Subsidiary Legislation
1.5.3	- Different Roles in MPF Business
1.5.4	- MPFA - History and Background
1.5.5	- MPFA - Regulatory Powers
1.5.6	- MPFA - Role and Composition
1.5.7	- MPFA - Relationship with Banks
1.6	**Hong Kong Monetary Authority – The Lead Regulator of Bank**
1.6.1	- HKMA - Regulatory Oversight of Other Financial Business of AIs
1.6.2	- Cooperation with Other Financial Regulators in Hong Kong
1.6.3	- Cooperation with Industrial Bodies in Hong Kong
1.6.4	- International Cooperation
1.6.5	- Professional Education through Educational Bodies
1.6.6	- Example of Regulatory Investigation with Other Financial Regulators
Chapter 2: Banking Supervision, Internal Policies, Standards and Guidelines	
2.1	**Supervisory Approach and CAMEL Rating**
2.1.1	- Supervisory Objectives
2.1.2	- Compliance with Basel Core Principles
2.1.3	- Supervisory Approach and Regulatory Expectations of the HKMA
2.1.4	- On-site Examination
2.1.5	- Offsite Review and Prudential Meeting
2.1.6	- Tripartite Meeting with External Auditors
2.1.7	- Sharing of Information with Other Supervisors
2.1.8	- Supervisory Framework
2.2	**Risk-Based Supervisory Approach**
2.2.1	- Introduction
2.2.2	- Key Objectives and Benefits of the Risk-Based Supervisory Framework
2.2.3	- Six-step Methodology
2.2.4	- Risk Assessment
2.2.5	- Eight Inherent Risks
2.2.6	- Sound Risk Management

2.3	**Hong Kong Monetary Authority and Hong Kong Exchanges and Clearing Limited – Corporate Governance Requirements**
2.3.1	- Definition of Corporate Governance
2.3.2	- Why is Corporate Governance important for AIs
2.3.3	- Principles of Corporate Governance
2.3.4	- Guidelines on Corporate Governance
2.3.5	- Responsibilities of the Board
2.3.6	- Structure and Functioning of the Board
2.3.7	- Performance Evaluation of the Board
2.3.8	- Corporate Governance Code – Listing Rules
2.3.9	- Example of a Corporate Governance Report of a Listed AI
2.4	**Risk Management System of AIs**
2.4.1	- Introduction
2.4.2	- Risk Governance
2.4.3	- Risk Appetite
2.4.4	- Management Policies, Procedures and Limits
2.4.5	- Risk Management Systems and Processes
2.4.6	- Internal Control System, Compliance and Internal Audit Functions
2.4.7	- Example – Risk Management Framework of a Listed AI
2.5	**Regulatory Expectation of Internal Controls System**
2.5.1	- Definition of Internal Control
2.5.2	- Purposes of Internal Control
2.5.3	- Internal Control Activities
2.5.4	- Key Regulatory Expectations of Internal Control
2.5.5	- Common Issues of Internal Control
2.5.6	- Example of an Internal Control Report of a Listed AI
2.5.7	- Example of Compliance controls
Chapter 3: Bank Culture Reform	
3.1	**Treat Customers Fairly Charter (2013)**
3.1.1	- Background
3.1.2	- TCF Charter Launching Ceremony (28 October 2013)
3.1.3	- Main Principles of TCF Charter (28 October 2013)
3.1.4	- TCF Charter for Private Wealth Management Industry (8 June 2017)
3.1.5	- From TCF Charter to Bank Culture Reform
3.2	**Bank Culture Reform Circular (2017)**
3.2.1	- Background
3.2.2	- Bank Culture Reform Circular (2 March 2017)
3.2.3	- Sound Bank Culture – Three Pillars
3.2.4	- Governance
3.2.5	- Incentive Systems
3.2.6	- Assessment and Feedback Mechanisms
3.2.7	- Implementation of the Culture Reform Requirements by AIs
3.43	**Supervisory Measures for Bank Culture**
3.3.1	- Supervision of Bank Culture Circular (19 December 2018)
3.3.2	- Major Supervisory Measures
3.3.3	- Self-assessment
3.3.4	- Focus Review
3.3.5	- Culture Dialogue
3.3.6	- Experience from Overseas Practices
3.4	**Self-assessment on Bank Culture Reform**
3.4.1	- Background

3.4.2	- Self-assessment – Purpose and AIs Covered
3.4.3	- Major Areas Assessed
3.4.4	- Report on Review of Self-assessments on Bank Culture
3.4.5	- Range of Practices and Common Themes of the AIs
3.4.6	- Next Steps for AIs
3.5	**Focus Review, Culture Dialogue and Industrial Survey**
3.5.1	- Focus Review on Incentive Systems
3.5.2	- Culture Dialogue with Bank – Incentive System, Staff Training and Internal Escalation of Culture Issues
3.5.3	- Industrial Survey – Opinion from Bank Employees
3.5.4	- Further Development and Follow-up Actions
Chapter 4: Major Statutory Requirements for Bank in Hong Kong	
4.1	**Banking Ordinance**
4.1.1	- Purposes of the Ordinance
4.1.2	- Major Provisions
4.1.3	- Regulatory Powers of the MA on AIs
4.1.4	- Authorisation for the Conduct of Banking Business and Business of Taking Deposits
4.1.5	- Approval of Controller, Chief Executive, Director, etc.
4.1.6	- Financial Disclosure, Reporting and Notification Requirements
4.1.7	- Liquidity Requirements
4.1.8	- Capital Requirements
4.1.9	- Limitations on Exposures and Interests of AIs
4.1.10	- Code of Practice and Guidelines on Business Practice
4.1.11	- Other Important Provisions in Part X of the BO
4.1.12	- Major Subsidiary Legislation
4.2	**Securities and Futures Ordinance**
4.2.1	- Purposes of the Ordinance
4.2.2	- Regulated Activities
4.2.3	- Major Provisions
4.2.4	- Regulatory Powers of the SFC
4.2.5	- Exchanges, Clearing Houses, Exchange Controllers, Investor Compensation Companies and Automated Trading Services
4.2.6	- Regulation of Offers of Investments
4.2.7	- Licensing and Registration of Intermediaries
4.2.8	- Business Conduct, Supervision and Investigation of Intermediaries
4.2.9	- Major Subsidiary Legislation
4.3	**Insurance Ordinance**
4.3.1	- Purposes of the Ordinance
4.3.2	- Insurance Activities Governed by the Ordinance
4.3.3	- Major Provisions
4.3.4	- Regulatory Powers of the IA
4.3.5	- Authorisation of and Regulatory Powers over Authorised Insurers
4.3.6	- Long Term Business and General Business
4.3.7	- Licensed Insurance Intermediaries
4.3.8	- Conduct Requirements of Licensed Insurance Intermediaries and Disciplinary Powers of the IA
4.3.9	- Major Subsidiary Legislation
4.4	**Mandatory Provident Fund Schemes Ordinance**
4.4.1	- Purposes of the Ordinance
4.4.2	- Major Provisions
4.4.3	- Regulatory Powers of the MPFA

4.4.4	- Mandatory Contributions of Employers and Employees of MPF Schemes
4.4.5	- Supervision of MPF Schemes
4.4.6	- Supervision of MPF Intermediaries
4.4.7	- Major Subsidiary Legislation
4.5	**Personal Data (Privacy) Ordinance**
4.5.1	- Background and Purpose of the Ordinance
4.5.2	- Six Data Protection Principles
4.5.3	- Regulatory Powers of the Privacy Commissioner for Personal Data ("PCPD")
4.5.4	- Engagement of AIs with the PCPD
Chapter 5: Regulatory Objectives and Relevant Mandates	
5.1	**Code of Banking Practice - annual self-assessment**
5.1.1	- Background and Objectives of the CoBP
5.1.2	- Applicability of the CoBP
5.1.3	- General Principles
5.1.4	- Major Recommendations on Banking Services
5.1.5	- Annual Compliance Self-assessment of the CoBP
5.1.6	- Published Results of the Self-assessment
5.1.7	- Non-Compliance with the CoBP and Follow-up
5.2	**Code of Conduct for Persons Licensed by or Registered with the Securities and Future Commission**
5.2.1	- Background and Purposes of the SFC Code
5.2.2	- Applicability of the SFC Code to AIs (as RI)
5.2.3	- General Principles
5.2.4	- Major Provisions
5.2.5	- Enforcement of the SFC Code by the SFC
5.2.6	- Non-Compliance with the Code and Follow-up
5.3	**Code of Conduct for Licensed Insurance Agents and Code of Conduct for Licensed Insurance Brokers**
5.3.1	- Background and Aims of the Codes
5.3.2	- Applicability of the Insurance Agent Code to AIs (as Insurance Agency)
5.3.3	- General Principles
5.3.4	- Major Provisions
5.3.5	- Enforcement of the Insurance Agent Code by the IA
5.3.6	- Non-compliance with the Insurance Agent Code and Follow-up
5.4	**Guidelines on Conduct Requirements for Registered Intermediaries (Issued by the Mandatory Provident Fund Schemes Authority)**
5.4.1	- Background and Purposes of the MPFI Guidelines
5.4.2	- Applicability of the MPFI Guidelines
5.4.3	- Minimum Standards
5.4.4	- Major Provisions
5.4.5	- Enforcement of the MPFI Guidelines by the MPFA
5.4.6	- Non-compliance with the MPFI Guidelines and Follow-up
Chapter 6: Introduction to International Regulation	
6.1	**International Regulations (Role of Regulators, Regulatory Powers and International Regulatory Models and Latest Market Trends)**
6.1.1	- Background of International Regulation
6.1.2	- Development of International Business and MNCs with Cross-border Business across Different Geographies
6.1.3	- Necessity for Regulations to be Applicable outside of the Country, e.g. AML/CTF Rules and Anti-tax Evasion Regulations
6.1.4	- Different International Regulatory Models: Single Country Regulation (e.g. FATCA) vs International Regulatory Standards (e.g. CRS/AEOI)

6.1.5	- Internationalisation of Business and Market Trends of International Regulatory Cooperation in Addressing International Regulatory Risks
6.2	**Foreign Account Tax Compliance Act ("FATCA")**
6.2.1	- Background and Purposes of FATCA
6.2.2	- Applicability of FATCA to Banks in Hong Kong
6.2.3	- FATCA Requirements for AIs and AIs' Customers
6.2.4	- Control and Operational Procedures for FATCA
6.2.5	- Non-participating Foreign Financial Institutions and Consequential Penalty Tax
6.2.6	- Challenges in Compliance with FATCA Requirements
6.3	**Common Reporting Standards (AEOI/CRS)**
6.3.1	- Background and Purposes of CRS/AEOI
6.3.2	- Inland Revenue (Amendment) (No.3) Ordinance (Cap. 112) 2016
6.3.3	- Applicability of CRS/AEOI in Hong Kong
6.3.4	- CRS/AEOI Requirements for AIs and AIs' Customers
6.3.5	- Control and Operational Procedures for CRS/AEOI
6.3.6	- Consequences of Non-Compliance with CRS/AEOI Requirements
6.3.7	- Challenges in Compliance with CRS/AEOI Requirements
6.4	**EU General Data Protection Regulation (GDPR)**
6.4.1	- Background and Purposes of the GDPR
6.4.2	- Extra-territorial Application of the GDPR and Applicability in Hong Kong
6.4.3	- Comparison between the PDPO and the GDPR
6.4.4	- Major Provisions of the GDPR Relevant to AIs and AIs' Customers in Hong Kong
6.4.5	- Data Privacy Governance, Data Mapping and Impact Assessment
6.4.6	- New and Enhanced Rights of Data Subjects
6.4.7	- Data Protection Seals, Codes of Conduct and Cross-jurisdiction Data Transfer
6.5	**FX Global Code / Volcker / MIFID**
6.5.1	- FX Global Code
6.5.2	- Volcker Rule
Chapter 7: Registration and Licensing Requirements	
7.1	**Banking Ordinance – AI, CE, ACE and Manager**
7.1.1	- Types of AI under the BO
7.1.2	- Minimum Criteria of the MA for Authorization of AIs
7.1.3	- Continuous Satisfaction with the Minimum Criteria for Authorization by AIs
7.1.4	- Requirements of Local Branch, Local Office and Overseas Branch
7.1.5	- Requirements of Foreign Bank Branch and Representative Office in Hong Kong
7.1.6	- Approval Requirements for CE, ACE and Director and Systems of Control for Appointment of Section 72B Manager
7.1.7	- Assessment Criteria of the MA on Approval for CE and Director
7.1.8	- Statutory Notification Requirement for Appointment of Section 72B Manager
7.2	**Securities and Futures Ordinance – Registered Institution and Relevant Individual**
7.2.1	- Registration Requirements for AI Carrying on RAs as RI under the SFO
7.2.2	- Requirements for Appointment of Two or More EOs for Each RA
7.2.3	- Fit and Proper Requirements for EO
7.2.4	- Fit and Proper Requirements for REI
7.2.5	- CPT Requirements for EO and REI
7.3	**Insurance Ordinance – Agency and Technical Representative**
7.3.1	- Licensing Requirements for AI as Licensed Insurance Agency under the IO
7.3.2	- Requirement for Appointment of an RO by a Licensed Insurance Agency
7.3.3	- Fit and Proper Requirements for RO
7.3.4	- Fit and Proper Requirements for Licensed Technical Representative (Agent) ("TR")
7.3.5	- CPD Requirements for RO and TR

7.4	**Mandatory Provident Fund Schemes Ordinance – MPF Intermediary**
7.4.1	- Registration Requirements for AI as PI under the MPFSO
7.4.2	- Requirement for Appointment of an RO by a PI
7.4.3	- Criteria of the MPFA for Approval of RO Appointed by a PI
7.4.4	- Registration Requirements for SI under the MPFSO
7.4.5	- CPD Requirements for RO and SI
7.5	**Listing Rules – Listed AIs**
7.5.1	- Background of the Rules - Listed AI
7.5.2	- Chapter 13 Equity Securities – Continuing Obligations
7.5.3	- Listing Rules on Debt Securities
7.5.4	- Chapter 24 Debt Securities - Application Procedures and Requirements
7.5.5	- Chapter 37 Debt Securities - Debt Issues to Professional Investors Only
7.5.6	- Appendix 14 Corporate Governance Code
7.5.7	- Compliance with the Rules
7.6	**Manager-in-charge (MIC) Regime – Applicability to AIs**
7.6.1	- Background of the SFC MIC Regime
7.6.2	- MICs Required for Licensed Corporation Licensed by the SFC
7.6.3	- Responsibilities and Legal Liabilities of MIC
7.6.4	- Management Structure Information for the SFC
7.6.5	- Application of the MIC Regime to AIs
7.6.6	- Ongoing Review and Monitoring of AIs' Compliance with the MIC Regime Requirements
Chapter 8: Regulatory Breach and Operational Risk Incident Management	
8.1	**Identification, Review and Classification of Incident**
8.1.1	- Definition of Operational Risk Incident
8.1.2	- Categories of Operational Risk Incident
8.1.3	- Identification of Operational Risk Incidents – Internal vs External Factors
8.1.4	- Internal Tools for Identification and Assessment of Operational Risk Incidents
8.1.5	- Incident Management Team ("IMT") – Operations, IT, Business, Communication and Compliance
8.1.6	- Incident Management Protocol – Based on Nature of Incident
8.2	**Response and Management of Operational Risk Incident – Internal Escalation**
8.2.1	- Incident Management Protocol – Introduction and Major Elements
8.2.2	- Establishment of the IMT and Fact Finding
8.2.3	- First Management Escalation – Impact Analysis and Impact Control Action
8.2.4	- Implementation of Impact Control Action and Monitoring of Impact Situation
8.2.5	- External Escalation and Notification – Regulator, Customer and Public
8.2.6	- First Incident Report – Management and Regulator(s) (Including Customer Impact and Root Cause Analysis)
8.3	**Response and Management of Operational Risk Incident - Remediation and Disclosure**
8.3.1	- Management Review and Approval for Customer Impact Remediation Plan and IT Solution to Root Cause
8.3.2	- Notification to Regulator of the Remediation Plan and IT Solution
8.3.3	- Execution of Remediation Plan and IT Solution with Ongoing Updates to Management and Regulator(s)
8.4	**Response and Management of Operational Risk Incident - Lesson Learnt and System Enhancement**
8.4.1	- Identification of Accountability of Staff, Processes and Departments - Proposal and Execution of the Action
8.4.2	- Overall Financial Impact Analysis and Lessons Learnt
8.4.3	- Final Incident Report – Management and Regulator(s)

8.4.4	- Management Review and Approval for the Completion of the Incident and Dissolution of IMT
8.5	**Operational Risk Incident Regulatory Reporting Requirement of the HKMA**
8.5.1	- HKMA's Operational risk and Breach Incident Reporting Requirements
8.5.2	- Responsibilities of Chief Operating Officer
8.5.3	- Classification of Incident – Nature, Breach and Customer Impact
8.5.4	- Same-Day Reporting
8.5.5	- Disclosure to Affected Customers and the Public
8.5.6	- Root Cause Analysis
8.5.7	- Accountability of the Incident – Staff, Processes and Departments
8.5.8	- Ongoing Updates
8.5.9	- Final Report
8.6	**Reputational Issue in Incident Management**
8.6.1	- Importance of the Reputation of AIs
8.6.2	- Key Drivers of Reputation of AIs
8.6.3	- Effective Reputation Risk Management Process
8.6.4	- Reputation Risk Management – Operational Risk Incident
8.6.5	- Operational Risk Incident – Protection of the Reputation of AIs
8.6.6	- Example of Reputation Event – AI Annual Report Disclosure
Chapter 9: Future Development in Banking and the Relevant Regulatory Requirements	
9.1	**Digital Banking and e-Banking Regulatory Requirements**
9.1.1	- Definition of E-banking
9.1.2	- Evolution of HKMA E-banking Requirements since 2000
9.1.3	- Inherent Risks of E-banking Business
9.1.4	- From Internet Banking to Mobile Banking
9.1.5	- Risk Management of E-banking Services
9.1.6	- Technology Outsourcing
9.1.7	- IT Security Assessment and Independent Assessment of New E-banking Services
9.1.8	- E-banking Incident Management and Reporting
9.1.9	- Example – Faster Payment Security Issue
9.1.10	- Artificial Intelligence and Machine Learning ("ML")
9.2	**Open API and Open Banking Development in Hong Kong**
9.2.1	- What is API Technology
9.2.2	- Definition of Open API for Banking
9.2.3	- Open API for Banking – Concept and Practice
9.2.4	- Open API Framework for the Hong Kong Banking Sector – Launch Approach of the HKMA
9.2.5	- Implementation of Open API Framework for the Hong Kong Banking Sector – Phases Launched – Phases I, II, III and IV
9.2.6	- Challenges ahead for Adoption of Open APIs for Banking in Hong Kong
9.2.7	- Open API Adoption in Banking – Experience in Other Countries
9.3	**Virtual Banking Licensing and Regulatory Development**
9.3.1	- What is a Virtual Bank
9.3.2	- Virtual Banks vs Conventional Banks
9.3.3	- Virtual Bank Authorisation Requirements
9.3.4	- Authorisation of Eight Virtual Banks in 2019
9.3.5	- Commencement of Business of Virtual Banks in 2020
9.3.6	- Virtual Bank – Business and Operational Risks
9.4	**Sustainable and Green Banking Business Development in Hong Kong**
9.4.1	- Background of Green and Sustainable Banking to Address Climate Risk

9.4.2	- HKMA's Key Measures in Addressing Climate Risk – Three Sets of Measures: Green and Sustainable Banking, Responsible Investment and Centre for Green Finance
9.4.3	- Establishment of Green and Sustainable Finance Cross-Agency Steering Group in May 2020
9.4.4	- Status of Development in Green and Sustainable Banking in Hong Kong as of June 2022
9.5	**Regulatory and Compliance Challenges from Sustainable and Green Banking Business**
9.5.1	- Establishment of Common Assessment Framework for Measurement of "Greenness Baseline" for AIs
9.5.2	- White Paper on Green and Sustainable Banking – June 2020
9.5.3	- Supervisory Expectations on Climate Resilience for AIs
9.5.4	- Establishment of Business and Risk Management Systems to Comply with the Supervisory Expectations on Climate Resilience for AIs
9.5.5	- HKMA Circular Dated 30 Jun 2022 on Embedding Climate Risk in Banking Supervision
Chapter 10: Case Studies – Compliance Challenge	
10.1	**Challenge of New Products and Services**
10.1.1	- Expectation of New Products and Services from Customers
10.1.2	- New Products and Services to Cope with Market Situation
10.1.3	- Ongoing Changes in the Channel of Delivery of Products and Services including Digital Channels
10.1.4	- Risks Associated with New Products and Services
10.1.5	- Risks Associated with Different Delivery Channels
10.1.6	- New Products and Services - Internal Review and Approval Process
10.1.7	- New Delivery Channel – Pre-launch Review and Assessment
10.1.8	- Regulatory Requirements to Meet the Fast Pace of Development of New Products and Services in the Financial Market
10.1.9	- Ongoing Enhancement of Business and Product Knowledge of the Risk and Compliance and Functions
10.2	**Challenge of Ongoing Changes in Regulatory Requirements**
10.2.1	- Background – Ongoing Evolution of Regulatory Requirements
10.2.2	- Changes of Regulatory Requirements – Demand Driven and Immediate
10.2.3	- Changes of Regulatory Requirements – Well-Planned and Medium to Long-Term
10.2.4	- Challenges in Compliance with the New Requirements
10.2.5	- Structural Changes in Internal Control and Operational Processes Take time
10.2.6	- IT System Enhancements – Costly and Take Time
10.2.7	- New Processes – Staff Training and Compliance Monitoring of Staff Adherence to the New Process
10.3	**Challenge of External Event**
10.3.1	- External Event – Impact on AIs' Business and Compliance with Regulatory Requirements
10.3.2	- Major Types of External Event Affecting AIs' Business
10.3.3	- Effects on Business Volume
10.3.4	- Effects on Ways of Conducting Business
10.3.5	- Effects on Products and Services Offered
10.3.6	- AIs to Cope with these effects - Additional Sales and Operational Processes
10.3.7	- Enhancement of Compliance Monitoring and Review to Cope with the Additional Sales and Operational Processes
10.4	**Case Study – Compliance Breach involving Staff Misconduct**
10.4.1	- Overview of the Staff Misconduct Case
10.4.2	- Identification of the Case - Customer Complaint, Sales Quality Review

10.4.3	- Analysis of the Case - Facts, Customer Detriment, Misconduct
10.4.4	- Reporting - Management, Regulator
10.4.5	- Investigation by Regulator and Conclusion - Staff Misconduct involving Regulatory Breach
10.4.6	- Sanctions on Staff
10.4.7	- Lessons Learnt - Implications for the AI
10.5	**Case Study – Operational Risk Incident with Major Customer Impact**
10.5.1	- Overview of the Operational Risk Incident Case
10.5.2	- Identification of the Case - IT Check
10.5.3	- Analysis of the Case - Facts, Customer Detriment, IT Issue
10.5.4	- Reporting to Regulator
10.5.5	- Investigation by Regulator and Conclusion - IT Operational Issue involving Regulatory Breach
10.5.6	- Sanctions on the AI and Remediation Work
10.5.7	- Lessons Learnt - Enhancement of IT System, Implications for the AI

D. Recommended Readings

Essential Readings:

1. HKIB Study Guide of ECF-ORM: Module 2 Regulatory Framework and Compliance in Banking Industry. (2025).

Supplementary Readings

1. Hong Kong Legislation. Chapter 155, Chapter 571, Chapter 41, Chapter 485 and Chapter 486.
2. Hong Kong Monetary Authority. (2022). Supervisory Policy Manual, Risk-based supervisory approach.
3. Hong Kong Monetary Authority. (2017). Supervisory Policy Manual, Corporate governance of locally incorporated authorized institutions.
4. Hong Kong Monetary Authority. (2017). Supervisory Policy Manual, Risk Management Framework.
5. Hong Kong Monetary Authority. (2018). Supervisory Policy Manual, Interest Rate Risk in the Banking Book.
6. Hong Kong Monetary Authority. (2022). Supervisory Policy Manual, Operational risk management.
7. Hong Kong Monetary Authority. (2017). Circular on Bank Culture Reform.
8. The Hong Kong Association of Banks/The DTC Association. (2023). Code of Banking Practice.
9. Securities and Futures Commission. (2024). Code of Conduct for Persons Licensed by or Registered with the Securities and Futures Commission.
10. Insurance Authority. (2019). Code of Conduct for Licensed Insurance Agents.

11. Competition Commission. (2015). Guideline on the First Conduct Rule and Guideline on the Second Conduct Rule.

Further Readings

1. Nil

6.3. Module 3: Fundamentals of Operational Risk Management and Risk Governance

A. Module Objective

The module aims to provide candidates with the concepts and building block of operational risk, the operational risk governance and framework. It also aims to equip the learners to adopt the operational risk principles into practice; execute the operational risk management cycle; and integrate with other risk functions to promote holistic view of risks.

B. Module Intended Learning Outcome

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

- Describe 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 organisation;
- Implement and practice the operational risk principles and define the operational risk appetite;
- Execute the operational risk assessment, measurement and reporting; and
- Apply and incorporate with technology, resiliency and enterprise risk assessment.

C. Syllabus

Chapter 1: Overview Of Operational Risk	
1.1	**Introduction**
1.2	**Definitions**
1.2.1	- Definition of Risk Management
1.2.2	- Importance of Risk Management
1.2.3	- Types of Operational Risks faced by the Bank
1.2.4	- Taking Risk as Integral Part of Banking
1.2.5	- Definition and Types of Inherent Risks
1.2.6	- CAMEL Process
1.2.7	- Risk Management System
1.2.8	- Risks in Banking and Financial Services
1.2.9	- Evolution of Operation Risk
1.2.10	- Business Lines of the Banking Industry
1.2.11	- Definition of Risk (ISO 31000)
1.2.12	- Difference between Certainty VS Risk VS Uncertainty
1.2.13	- Definition of Operational Risk
1.2.14	- Operations Risk VS Operational Risk
1.2.15	- Inherent Risk VS Residual Risk
1.2.16	- Preview on Top 10 Operational Risks
1.2.17	- Top Operational Risk Issues Discussed in Board Room
1.2.18	- Operational Risk Management Framework
1.2.19	- FDIC 2024 Operational Risk Review
1.3	**Drivers**
1.3.1	- Benefits of Operational Risk Management
1.3.2	- Value of Operational Risk Management

1.3.3	- Key Deliverables of Sound Operational Risk Management
1.3.4	- Drivers of Good Operational Risk Management
1.3.5	- Lesson Learnt on Drivers Leading to 2008 Financial Crisis
1.3.6	- Reasons Leading to Management of Operational Risk
1.3.7	- Key Internal Operational Risk Drivers
1.3.8	- Categories of Operational Risk Drivers
1.3.9	- Operational Risk Causal Factors
1.3.10	- Process Factors
1.3.11	- People Factors
1.3.12	- System Factors
1.3.13	- External Factors
1.3.14	- Other Specific Operational Risk Drivers – Culture and Strategy
1.3.15	- Other Specific Operational Risk Drivers – Regulators and M&A
1.3.16	- Other Specific Operational Risk Drivers – Best Practice and Risk Aggregation
1.3.17	- Other Specific Operational Risk Drivers – New Products and Performance & Resource Allocation
1.3.18	- Expectation from Stakeholders
1.3.19	- Use of Operational Risk in Decision Making
1.3.20	- Positioning Operational Risk as Business Enabler
1.4	**Different Types**
1.4.1	- Risk Taxonomy
1.4.2	- Topology of Financial Risks
1.4.3	- Basel Level of Categorisation of Operational Risk
1.4.4	- Basel Categories of Business Lines
1.4.5	- Basel Categories of Event Types
1.4.6	- Typical Types Operational Risks
1.4.7	- Current Market Development that Requires Risk Attention
1.4.8	- Factors Leading to Operational Risk Vulnerabilities
1.4.9	- Samples of Major Prominent Operational Risk Events by Business Functions
1.4.10	- Iceberg Model
1.5	**Risk Analysis Model – Cause, Events, Impact**
1.5.1	- Swiss Cheese Model
1.5.2	- Operational Risk Event and Causal Effects
1.5.3	- ORX Extended Causes and Impact Model
1.5.4	- ORX Operational Loss Industry Pattern
1.5.5	- ORX Extended Causes and Impact Model
1.5.6	- ORX Causes Categories
1.5.7	- ORX Event Categories
1.5.8	- ORX Impact Categories
1.5.9	- Risk Management Sequence
1.6	**Relationship with Other Risk Functions**
1.6.1	- Recap on Risks in Bank
1.6.2	- Linkage of Different Risks to the Risk Event and Impact
1.6.3	- Boundaries of Operational Risk
1.6.4	- Structural Differences between Risk Types
1.6.5	- Risk Relationships and Interconnectivity
1.6.6	- Risk Boundaries – Operational Risk and Credit Risk Examples
1.6.7	- Risk Boundaries – Operational Risk and Market Risk Examples
1.6.8	- Differences between Operational Risk and other types of risks
1.6.9	- Identification – Unit of Measure
1.6.10	- Quantification / Measurement
1.6.11	- Mitigation / Control
1.6.12	- Comparisons between Operational Risk, Market Risk, and Credit Risk Management
1.6.13	- Integrating Related Disciplines in Banks

1.6.14	- Good Risk DNA
1.6.15	- Cooling-off Period for Unsecured Consumer Credit Products
1.7	**Case Studies**
1.7.1	- Case Study: Unauthorized Trading
1.7.2	- Case Study: Staff Embezzlement
1.7.3	- Case Study: Breach of Fiduciary Duties
1.7.4	- Case Study: Leakage of Customer Data
1.7.5	- Case Study: Letters of Credit Card Fraud
1.8	**Best Practice Guidance**
1.8.1	- Use of Risk Exposure Indicators
1.8.2	- Risk Management Adoption Maturity Model
1.8.3	- Looking Forward Risk Radars
Chapter 2: Operational Risk Framework and Governance	
2.1	**Introduction**
2.2	**Risk Governance Structure**
2.2.1	- Operational Risk Management Framework
2.2.2	- Key Recent Regulatory Changes (CG-1, IC-1)
2.2.3	- HKMA Revision to Risk Management Module IC-1
2.2.4	- Elements of a Sound Risk Management System
2.2.5	- General Components of Operational Risk Framework
2.2.6	- ORM Frameworks and Goals
2.2.7	- Corporate Governance
2.2.8	- Operational Risk Governance
2.2.9	- Typical Operational Risk Governance Structure Diagram
2.2.10	- Risk Culture and Operational Risk Governance
2.2.11	- Operational Risk Leadership
2.2.12	- Modes of Accountability
2.3	**Three Lines of Defence**
2.3.1	- Three Lines of Defense
2.3.2	- Responsibilities of Three Lines of Defense
2.3.3	- Evolution of 1.5 Line
2.3.4	- Three Lines of Defence Approach
2.3.5	- An Alternative ‘Blended’ Approach
2.3.6	- Three Lines of Defence Partnership Model
2.3.7	- Institute of Internal Auditors (IIA)’s Three Lines Model
2.3.8	- Effective Lines of Defense
2.4	**Roles and Responsibilities**
2.4.1	- Roles and Responsibilities
2.4.2	- Role of Board and Senior Management
2.4.3	- Role of Business and Support Units – 1st LOD
2.4.4	- Role of Corporate Operational Risk Function (CORF) – 2nd LOD
2.4.5	- Role of Corporate Subject Matter Specialists – Part of 2nd LOD
2.4.6	- Communication, Consultation and Collaboration Among the Three Lines
2.4.7	- Operational Risk Committee
2.4.8	- Points of Escalation to Various Committees
2.5	**Risk Culture and Indicators**
2.5.1	- Definition of Risk Culture
2.5.2	- Levels of Risk Culture
2.5.3	- Risk Sub-Culture
2.5.4	- Assessing Risk Culture
2.5.5	- Definition of Operational Risk Culture
2.5.6	- Attitudes, Behaviours and Culture
2.5.7	- Importance of Risk Culture
2.5.8	- Risk Culture (Principle 1 of PSMOR)

2.5.9	- Risk Culture Aspects Model
2.5.10	- Some Indicators of Good Risk Culture
2.5.11	- Monitoring Risk Culture: Risk Culture Metrics
2.5.12	- Monitoring Risk Culture: Risk Culture Metrics - Example
2.5.13	- Influencing Risk Culture
2.5.14	- Implication on Strategy and Leadership (Including Tone)
2.5.15	- Implication on Risk Appetite and Tolerance
2.5.16	- Implication on HR Policies and Procedures
2.5.17	- Implication on Communication: Formal and Informal
2.5.18	- Implication on Process and System Design
2.5.19	- Implication on Risk Governance
2.5.20	- Reflection on HKMA Bank Culture Self Assessment
2.6	**Risk Governance on Handling of Emerging Risk**
2.6.1	- Definition of Emerging Risks
2.6.2	- Interconnection of Risks
2.6.3	- Typology of Uncertainties
2.6.4	- Types of Emerging Risk
2.6.5	- ORX 2019 Top Emerging Risks
2.6.6	- Emerging Risk Trend
2.6.7	- Emerging Risk Radar
2.6.8	- Projection of Emerging Top Risks
2.6.9	- Emerging Risk – Cyber Risk
2.6.10	- Emerging Risk – Emerging Technology
2.6.11	- Emerging Risk – Climate Risk Hazards
2.6.12	- Emerging Risk Framework
2.6.13	- Drivers of Emerging Operational Risks
2.6.14	- Contributing Factors to Emerging Operational Risk
2.6.15	- Governance of Emerging Risk
2.6.16	- Risk Biases Leading to Hidden Emerging Risks
2.6.17	- Identification of Emerging Risks and Opportunities
2.6.18	- Tools for Identification of Emerging Risks
2.6.19	- Increasing Awareness of Potential Risks
2.6.20	- Risk Velocity
2.6.21	- Action on Emerging Risk
2.6.22	- Solution to Overcome Risk Biases
2.6.23	- 3rd Line Perspective: ECIIA Top Risk Survey
2.6.24	- Monitoring and Improvement of Emerging Risks Management
2.7	**Case Studies**
2.7.1	- Case Study: Misappropriation of an AI's money by a staff member
2.8	**Best Practice Guidance**
2.8.1	- Building Blocks of Operational Risk Culture
2.8.2	- Embedding Risk in Business Strategy
Chapter 3: Operational Risk Principles and Appetite	
3.1	**Introduction**
3.2	**Principles of Operational Risk Management Framework and Implementation**
3.2.1	- Basel Consultative Paper – Revisions to Principles for the Sound Management of Operational Risk (PSMOR)
3.2.2	- Structure of Principles for the Sound Management of Operational Risk
3.2.3	- Key Objectives of Operational Risk Principles
3.2.4	- Summary of the 12 Basel PSMOR
3.2.5	- Role of Supervisors
3.2.6	- Deep Dive on Operational Risk Framework (Principle 2 of PSMOR) - Framework
3.2.7	- Deep Dive on Operational Risk Framework (Principle 3 of PSMOR) - Governance
3.2.8	- Principles for Effective Risk Management (ISO 31000)

3.2.9	- Stages of ORM Implementation in Banks
3.2.10	- Commencement of Basel III Final Reform Package
3.2.11	- Revised Pillar 3 Disclosure Package
3.3	**Risk Control and Mitigation**
3.3.1	- Definition of Internal Controls
3.3.2	- Deep Dive on Control and Mitigation (Principle 9 of PSMOR)
3.3.3	- HKMA Requirement on Internal control System
3.3.4	- Internal Control Model
3.3.5	- Several Typical Operational Risks in Business Processes and the Related Control Measures
3.3.6	- Internal Control System
3.3.7	- Types of Internal Controls
3.3.8	- Definition of Control Testing
3.3.9	- Types of Internal Control Testing
3.3.10	- Risk Based Internal Control Testing
3.3.11	- Active Failures and Latent Conditions
3.3.12	- Effect of Internal Controls on Risks
3.3.13	- Effectiveness of Controls
3.4	**Operational Risk Planning and Processes**
3.4.1	- Operational Risk Planning
3.4.2	- Overview of Operational Risk Management Process
3.4.3	- Operational Risk Management Process
3.4.4	- Operational Risk Management Process-Broad Steps
3.4.5	- Operational Risk Management Actions and Tools
3.4.6	- The Bow Tie Diagram
3.4.7	- Operational Risk Event, Cause and Effect
3.4.8	- “Swiss Cheese” Model of Defences
3.5	**Operational Risk Appetite Framework**
3.5.1	- Definition of Operational Risk Appetite
3.5.2	- Benefits of Operational Risk Appetite
3.5.3	- Focus of Operational Risk Appetite
3.5.4	- Operational Risk Tolerance
3.5.5	- Determination of Operational Risk Appetite and Risk Tolerance
3.5.6	- The R&R of the Board on the Determination
3.5.7	- The R&R of the Business Management on the Determination
3.5.8	- The R&R of the Internal Audit on the Determination
3.5.9	- Diagrammatic Explanation of Risk Appetite Funnel
3.5.10	- Top-down and Bottom-up Approaches to Setting the Appetite
3.5.11	- Alignments of the Frameworks to the Different Forms of Risk Appetite Expression
3.5.12	- Expressing the Operational Risk Appetite (ORA) Quantitatively and Qualitatively
3.5.13	- Deciding on the Appropriate Level of the ORA and Risk Tolerances
3.5.14	- Implementing the ORA and Tolerances
3.5.15	- Aggregation and Reporting
3.5.16	- Management and Decision Making
3.5.17	- Sample Operational Risk Appetite Template
3.5.18	- Structure of Actionable Risk Appetite
3.5.19	- Consistent Operational Risk Appetite
3.5.20	- Articulating Operational Risk Appetite
3.5.21	- Defining Operational Risk Appetite
3.5.22	- Setting Operational Risk Appetite and Tolerance
3.5.23	- Setting Operational Risk Appetite Thresholds
3.5.24	- Setting and Application
3.5.25	- Market View on Operational Risk Appetite
3.5.26	- Operational Risk Assessment for New Business, Product, and Changes

3.5.27	- Operational Risk Heatmap
3.5.28	- Background, Methodology, and Deliverables of the Critical Operational Risk Registers
3.5.29	- Examples of Operational Risk Appetite Statements
3.6	**Operational Risk Impact**
3.6.1	- Developing Assessment Criteria
3.6.2	- Sample of Operational Risk Rating Scale
3.6.3	- ORX Impact Categories
3.7	**Case Studies**
3.7.1	- Case Study: Ineffective Call-back Verification on Third-party Fund Transfer
3.8	**Best Practice Guidance**
3.8.1	- Best Practice Principles on Operational Risk Appetite
3.8.2	- Internal Controls (Control Environment and Business Process Controls)
3.8.3	- Interaction between Operational Risk Management Tools
3.8.4	- Operational Risk Management Tools Metrics
Chapter 4: Operational Risk Assessment, Measurement And Reporting	
4.1	**Introduction**
4.2	**Operational Risk Assessment**
4.2.1	- Stages of Operational Risk Assessment Process
4.2.2	- Methods for Assessing Risks
4.2.3	- Identifying Operational Risk
4.2.4	- Tools of Operational Risk Assessment
4.2.5	- Benchmarking for Identification
4.2.6	- Risk Factors for Consideration
4.2.7	- HKMA Requirement on Operational Risk Assessment Methods
4.3	**Quantification of Operational Risk**
4.3.1	- Explanation of Quantification of Operational Risk
4.3.2	- Value at Risk (VaR)
4.3.3	- Conditional VaR
4.3.4	- Extreme Value Theory
4.3.5	- Peaks-over-Threshold
4.3.6	- Fuzzy Logic
4.3.7	- Bayesian Belief Network
4.3.8	- Artificial Neural Networks
4.3.9	- Bootstrapping
4.3.10	- Heat Map
4.3.11	- Risk Registers
4.3.12	- Practical Consideration
4.4	**Risk Reporting and Dashboard**
4.4.1	- Objectives of Operational Risk Reporting
4.4.2	- Factors of Operational Risk Reporting
4.4.3	- Process of Operational Risk Reporting
4.4.4	- Typical Contents of Operational Risk Reports
4.4.5	- Timeliness of Operational Risk Reports
4.4.6	- Features of Operational Risk Reporting
4.4.7	- Types of Operational Risk Reporting
4.4.8	- Action of Operational Risk Reporting
4.4.9	- Best Practice Principles of Operational Risk Reporting
4.4.10	- Critical Success Factors of Operational Risk Reporting
4.4.11	- Examples of Operational Risk Reports
4.4.12	- Checkpoints on Good Operational Risk Reporting
4.5	**Nature of The Financial Products**
4.5.1	- Overview of Financial Service Products
4.5.2	- Funds Intermediation Products
4.5.3	- Transaction Intermediation Products

4.5.4	- Information Intermediation Products
4.5.5	- Risk Intermediation Products
4.5.6	- Work Activity Related to Financial Services Products
4.5.7	- Managing Risk in New Product Development
4.5.8	- Key Features of Equity
4.5.9	- Demonstrate Understanding of Equity
4.5.10	- Key Features of Various Types of Bonds
4.5.11	- International Bond Markets
4.5.12	- Major Categories of Money Market Products
4.5.13	- Differences and Similarities between the Major Types of Cash Money Market
4.5.14	- The Major Commodity Categories
4.5.15	- Major Categories of Derivative Products
4.5.16	- The Markets where Major Categories of Derivative Products Are Usually Traded
4.5.17	- Major Categories of Alternative Investments
4.6	**Common Risk Types**
4.6.1	- Types of Operational Loss
4.6.2	- Types of Categorisation of Operational Risk
4.6.3	- Rationale for Operational Risk Categorisation
4.6.4	- Key Principles for Categorising Operational Risks
4.6.5	- Designing an Operational Categorisation Framework
4.6.6	- Minimising Gaps and Overlaps
4.6.7	- Improving Granularity
4.6.8	- Implementation – Roles and Responsibilities
4.6.9	- Implementation – Ensuring Consistent Use
4.6.10	- Implementation – Reporting
4.6.11	- Implementation – Addressing Boundary Events
4.6.12	- Common Risk Types of Services and Products
4.6.13	- Typology of Operational Risks
4.7	**Case Studies**
4.7.1	- Case Study: Mistake in Allowing an Authorized Person to Bring in Another Person when Accessing a Safe Deposit Box
4.8	**Best Practice Guidance**
4.8.1	- Theme and Metrics for Conduct Risk Reporting
4.8.2	- Example of Conduct Risk Metrics Reporting
Chapter 5: Technology, Resiliency And Enterprise Risk Assessment	
5.1	**Introduction**
5.2	**Technology Risk Framework**
5.2.1	- Operational Risk in Information Technology
5.2.2	- Regulations for Technology Management in Banking Industry
5.2.3	- Managing Information and Communication Technology
5.3	**Cybersecurity**
5.3.1	- Typology of Information Security Risk
5.3.2	- Types of Cyber Security Threats
5.3.3	- Sample of Information Security Risk Assessment
5.3.4	- Key Controls in Information Security
5.3.5	- Sample of KRI in Information Security
5.3.6	- Cybersecurity Standards
5.3.7	- Information Security Management System
5.3.8	- ISO/IEC 27001 Information Security Management Systems Standard
5.3.9	- Sharing of Cyber-threat Information
5.3.10	- Principal Cyberactivities that are Criminalised by the Law
5.3.11	- Information Security Challenges Associated with Cloud Computing
5.3.12	- Cybersecurity Laws Affect Foreign Organisations
5.3.13	- Additional Cybersecurity Protections Beyond What Is Mandated by Law

5.3.14	- Government Incentivize Organizations to Improve Their Cybersecurity
5.4	**Data Privacy**
5.4.1	- Overview of Data Privacy
5.4.2	- Regulation on Data Privacy PDPO
5.5	**System Change Control**
5.5.1	- Risk Management in Change
5.5.2	- Quality Assurance, Testing, and Change Management
5.6	**Resiliency Risk**
5.6.1	- Definition of Resiliency
5.6.2	- Threats to Financial Resilience
5.6.3	- Interconnects of Financial and Operational Resiliency
5.6.4	- Drivers of Operational Resilience
5.6.5	- Risk, Resilience and Sustainability
5.6.6	- Managing Business Continuity Planning
5.6.7	- Business Continuity Management
5.7	**Types of Disasters**
5.7.1	- Types of Disasters
5.7.2	- Classification of Disasters
5.7.3	- Disasters VS Catastrophes
5.8	**Business Impact Analysis Overview**
5.8.1	- Definition of Business Impact Analysis
5.8.2	- Analysis of Business Impact Analysis
5.8.3	- Business Impact Analysis VS Risk Assessment
5.8.4	- HKMA Requirement on Business Impact Analysis
5.9	**Resiliency Plan**
5.9.1	- Definition of Business Continuity
5.9.2	- Roles and Responsibilities of Business Continuity Management
5.9.3	- Components of Business Continuity Management
5.9.4	- BCM Lifecycle
5.9.5	- Contingency Planning
5.10	**Plan Testing Overview**
5.10.1	- HKMA Requirement on Contingency Planning Testing
5.10.2	- HKMA Requirement on Contingency Planning Maintenance
5.11	**Enterprise Risk Framework**
5.11.1	- Overview of Enterprise Risk Management
5.11.2	- Definition of Enterprise Risk Management
5.11.3	- HKMA Requirement on Firm-wide Risk Management
5.11.4	- COSO Enterprise Risk Management Framework
5.11.5	- New COSO ERM - Integrating with Strategy and Performance
5.11.6	- Capability of Enterprise Risk Management
5.11.7	- Key Elements of an Effective Operational Risk within ERM Framework
5.11.8	- Integration of ORM Framework into ERM
5.12	**Enterprise Risk Appetite**
5.12.1	- Enterprise Risk Appetite
5.12.2	- Roles and Responsibilities in Risk Appetite Framework
5.12.3	- HKMA Requirement on Enterprise Risk Appetite Framework
5.13	**Enterprise Risk Limit**
5.13.1	- Enterprise Risk Limit
5.13.2	- Best Practice on Enterprise Risk Limit
5.13.3	- Structure on Enterprise Risk Limit
5.13.4	- HKMA Requirement on Enterprise Risk Limit
5.14	**Case Studies**
5.14.1	- Case Study: Misappropriation of a Customer's Funds by a Staff Member Using a Returned ATM Card

5.15	**Best Practice Guidance**
5.15.1	- The Main Industry Standards and Codes of Practice Promoting Cybersecurity (HKMA, SFC, IA, OGCIO, PCPD)
Chapter 6: Integrated Case Studies And Best Practices	
6.1	**Integrated Case Studies**
6.1.1	- Case Study: The Collapse of Barings Bank 1995
6.1.2	- Case Study: Safety Deposit Boxes at DBS
6.1.3	- Case Study: Société Générale Taken to the Brink
6.1.4	- Lessons Learnt from Risk Cases
6.2	**Best Practice Guidance**
6.2.1	- Ten Principles of the Best Practices in ORM

D. 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. (2025). Fundamentals of Operational Risk Management and Risk Governance.

Supplementary Readings

1. Basel Committee. (2021). Revisions To The Principles For The Sound Management Of Operational Risk.
2. Basel Committee. (2020). The Basel Framework: Frequently Asked Questions.
3. Basel Committee. (2021). Principles For Operational Resilience.
4. Basel Committee. (2019). Launch Of The Consolidated Basel Framework.
5. Basel Committee. (2018). Sound Practices: Implications Of Fintech Developments For Banks And Bank Supervisors.
6. Basel Committee. (2017). Basel III: Finalising Post-Crisis Reforms.
7. Hong Kong Monetary Authority. (2019). TM-E-1: Risk Management of E-Banking.
8. Hong Kong Monetary Authority. (2017). IC-1: Risk Management Framework.
9. Hong Kong Monetary Authority. (2022). OR-1: Operational Risk Management in Supervisory Policy Manual.
10. Hong Kong Monetary Authority. (2022). TM-G-2: Business Continuity Planning.
11. Hong Kong Monetary Authority. Operational Incidents Watch.
12. Hong Kong Monetary Authority. (2020). Report on Review of Self-assessments on Bank Culture.
13. Hong Kong Monetary Authority. (2018). Supervision for Bank Culture.
14. Hong Kong Monetary Authority. (2017). Bank Culture Reform.

Further Readings

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

6.4. Module 4: Advanced Operational Risk Management

A. Module Objective

This module 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 operational risk management function that take up a majority of responsibility in the operational risk management and business function risk and control.

B. 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 establisheffective 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 identifypotential operational risk events and assess their potential impact;
- Analyse 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 onfindings of operational risk events; and
- Design and deliver operational risk training to business units.

C. Syllabus

Chapter 1: Operational Risk Assessment Methodology And New Products Risk Assessment	
1.1	**Introduction**
1.2	**Risk Assessment Criteria**
1.2.1	- Optimal Risk Taking for Banks
1.2.2	- Stages for Risk Assessment Process
1.2.3	- Critical Risk Factors in Various Business Area
1.2.4	- Operational Risk Assessment Methods
1.2.5	- Operational Risk Assessment Requirements
1.2.6	- Operational Risk Assessment Tools
1.2.7	- Operational Risk Assessment Factors

1.2.8	- Operational Risk Management Cycle
1.2.9	- Timeliness of Operational Risk Assessment
1.2.10	- Operational Risk Assessment Process Map
1.2.11	- Developing Assessment Criteria
1.2.12	- Operational Risk Rating Scale (Sample)
1.3	**Risk Taxonomy**
1.3.1	- Operational Risk Taxonomy
1.3.2	- Development of Operational Risk Taxonomy
1.3.3	- Objective and Benefits of Operational Risk Taxonomy
1.3.4	- Value of Operational Risk Taxonomy
1.3.5	- Risk Taxonomy Hierarchy
1.3.6	- Taxonomy by Business Lines
1.3.7	- Taxonomy by Operational Risk Event Types
1.3.8	- Taxonomy by Operational Risk Causes
1.3.9	- Taxonomy by Operational Risk Loss Effects
1.3.10	- Taxonomy by Control Categories
1.3.11	- Operational Risk Taxonomy Mapping
1.3.12	- Basel Taxonomy Activity Examples (Level 3) – Loss Event Type Classification
1.3.13	- Best Practice: ORX Operational Risk Taxonomy
1.3.14	- Connection of the ORX Reference Taxonomy to the Basel Event Types
1.3.15	- ORX Reference Taxonomy
1.3.16	- ORX Bow Tie Method
1.3.17	- ORX Reference Taxonomy
1.3.18	- Top-level Observations From The Data
1.4	**New Process Change Risk Assessment**
1.4.1	- Manage Business Process Change Process
1.4.2	- Types of Business Process Changes
1.4.3	- Change Management R&R - First Line
1.4.4	- Change Management R&R - Second Line
1.4.5	- Business Process Change Scorecard
1.4.6	- Points of Risk Consideration (Example)
1.4.7	- Risk Assessment Thresholds for Business Process Change
1.4.8	- Operational Risk Perspective on Change
1.4.9	- Challenges on Risk Management for Changes
1.4.10	- Cohorts in Responding to Change
1.4.11	- Common Causes of Change Failure
1.4.12	- Information Requirement on Change
1.4.13	- Stage Involvement of Risk Function
1.4.14	- KRI for Monitoring Project Risks
1.5	**New Product Risk Assessment Cycle**
1.5.1	- New Product Definition
1.5.2	- Industry Observation on New Product
1.5.3	- Drivers for New Product
1.5.4	- Features of New Product
1.5.5	- Categorisation of New Product
1.5.6	- New Product Development Lifecycle
1.5.7	- New Product Risk Assessment Requirement
1.5.8	- Examples of Significant Changes to Risk Profile of Product (HKMA Illustration)
1.5.9	- Principles Governing the New-Product-Approval Process
1.5.10	- Issues on Managing New Product
1.5.11	- Types of Risks in New Process
1.5.12	- New Product Policy (Sample)
1.5.13	- New Product Committee (NPC)
1.5.14	- KRI for New Product

1.5.15	- New Product Risk Rating (NPRR)
1.5.16	- New Product Documentation
1.5.17	- New Product Risk Roles and Responsibilities – First Line
1.5.18	- New Product Risk Roles and Responsibilities – Second Line
1.5.19	- Product Expiration
1.5.20	- Consideration of Conflict of Interest
1.5.21	- Customer Onboarding
1.5.22	- Key Process and Regulatory Requirements of Customer Onboarding
1.5.23	- Risk Mitigation of Customer Onboarding
1.6	**Offboarding and Periodic Review**
1.6.1	- Factors for Product Offboarding
1.6.2	- Overview of Post Implementation Review
1.6.3	- Scope of Post Implementation Review
1.6.4	- Overview of Periodic Product Review
1.6.5	- Scope of Periodic Product Review
1.6.6	- Customer Offboarding
1.6.7	- Key Process and Regulatory Requirement of Customer Offboarding
1.6.8	- Risk and Mitigation of Customer Offboarding
1.6.9	- Latest Trend of Customer Onboarding and Offboarding
1.7	**Case Studies**
1.7.1	- Case Study: Mis-selling of Investment Products
1.7.2	- Case Study: Deficient practices in ascertaining insurance protection for bill discounting business
1.7.3	- Case Study: Underpayment of stamp duty for certain OTC transactions
1.8	**Best Practice Guidance**
1.8.1	- New Product Checklist (Sample)
Chapter 2: Scenario Analysis And Stress Testing	
2.1	**Introduction**
2.2	**Stress Testing**
2.2.1	- Definition of Scenario Analysis, Stress Testing and Reverse Stress Testing
2.2.2	- Relationship between Scenario Analysis, Stress Testing and Reverse Stress Testing
2.2.3	- Demarcating Scenario Analysis, Stress and Reverse Stress testing
2.2.4	- Overview and Risk Factors of Operational Risk Stress Testing
2.2.5	- Value of Operational Risk Stress Testing
2.2.6	- Elements of Operational Risk Stress Testing
2.2.7	- Types of Risks Covered in Stress Testing
2.2.8	- Guiding Principles of Stress Testing
2.2.9	- Purpose of Stress Testing and Scenario Analysis
2.2.10	- Features of Stress Testing and Scenario Analysis
2.2.11	- Benefits of Stress Testing and Scenario Analysis
2.2.12	- Linkage to Capital Planning Process
2.2.13	- Relationship between Sensitivity Analysis, Scenario Analysis, Stress Testing, Reverse Stress Testing, and Back Testing
2.3	**Scenario Analysis**
2.3.1	- Overview of Scenario Analysis
2.3.2	- Conducting Effective Scenario Analysis
2.3.3	- Identifying and Agreeing the Focus of Analysis
2.3.4	- Determining the Level of Analysis
2.3.5	- Key Components of Scenario Analysis Framework
2.3.6	- Scenario Design and Scenario Execution
2.3.7	- Approach in Developing Scenario Analysis
2.3.8	- Governance and Responsibilities
2.4	**Selection of The Scenarios**
2.4.1	- Animal Kingdom of Risks

2.4.2	- Black Swam Examples
2.4.3	- Gray Rhino Examples
2.4.4	- Questions on Understanding the Unknowns
2.4.5	- Steps in Building Scenario Analysis
2.4.6	- Relevance of Scenario Analysis
2.4.7	- Forward-looking Focus
2.4.8	- Data Collection
2.4.9	- Scenario Risk Drivers
2.4.10	- Scenario Distribution
2.4.11	- High Severity Scenario Examples
2.4.12	- Scenario Biases
2.4.13	- Possible Relationships between Operational Losses and Macroeconomic Conditions for Basel Event Types
2.4.14	- Identifying and Approving a Portfolio of Scenarios
2.4.15	- Techniques for Identifying Scenarios
2.4.16	- Sample of Common Scenarios (Corporate Bank)
2.4.17	- Assessing COVID Impact with Scenario Analysis
2.5	**Execution and Analysis**
2.5.1	- Running a Scenario Workshop
2.5.2	- Causes of Scenarios
2.5.3	- Assessing Impacts
2.5.4	- Assessing Likelihood
2.5.5	- Management Response
2.5.6	- Scenario Template
2.5.7	- Expert Assessment and Biases
2.5.8	- Validation and Governance
2.5.9	- Preparing for Operational Risk Workshop
2.5.10	- Conducting a Workshop
2.5.11	- The Participants
2.5.12	- Assessing Probability and Impact
2.5.13	- Workshop Analysis Techniques
2.5.14	- Validation of Output
2.5.15	- Governing the Process
2.5.16	- Making Effective Use of the Outputs
2.5.17	- Risk and Capital Modeling
2.5.18	- Calculating Baseline Loss
2.5.19	- Expected Levels of Loss
2.5.20	- Unexpected Levels of Loss
2.5.21	- Key Challenges in Scenario Analysis
2.6	**Benchmarking with The Industry**
2.6.1	- Industry Benchmarking of Scenario Analysis
2.6.2	- Industry Survey on Scenario Analysis
2.7	**Regulatory Guideline**
2.7.1	- Global Regulatory Timeline
2.7.2	- BCBS Principles for Sound Stress Testing Practices and Supervision
2.7.3	- HKMA Requirement on Stress Testing and Operational Risk Scenario Analysis
2.8	**Case Studies**
2.8.1	- Case Study: Phishing emails and fraudulent bank websites stealing customers' e-banking account information
2.9	**Best Practice Guidance**
2.9.1	- Stress Testing Toolkit
2.9.2	- Reverse Stress Testing Methodology
2.9.3	- Backtesting for Operational Risk
Chapter 3: Key Risk Indicators	

3.1	**Introduction**
3.2	**Difference Between Key Risk Indicator, Key Control Indicator and Key Performance Indicator**
3.2.1	- Definitions of Operational Risk Indicators
3.2.2	- Risk Indicators
3.2.3	- Control Indicators
3.2.4	- Performance Indicators
3.2.5	- Dimensions and Types of Key Risk Indicators
3.2.6	- KRI vs KCI vs KPI
3.2.7	- Composite Indicators
3.2.8	- Essentials of Key Indicators
3.2.9	- Categories of Key Risk Indicators
3.2.10	- Exposure Indicators
3.2.11	- Failure Indicators
3.2.12	- Stress Indicators
3.2.13	- Causal Indicators
3.2.14	- BCBS Principles
3.3	**Design**
3.3.1	- Life Cycle of Key Risk Indicators
3.3.2	- Roles of Key Risk Indicators
3.3.3	- Translating Risk Appetite
3.3.4	- Risk Monitoring
3.3.5	- Governance and Assurance
3.3.6	- Risk Assessment and Modelling
3.3.7	- Relevance
3.3.8	- Measurable
3.3.9	- Leading vs Lagging Indicators
3.3.10	- Types of Indicators
3.3.11	- Bow Tie Diagram for Key Risk Indicators
3.3.12	- Easy to Collect and Monitor
3.3.13	- Comparable
3.3.14	- Auditable
3.3.15	- Selecting Indicators: Top Down or Bottom Up
3.3.16	- Consideration for Top-down Approach
3.3.17	- Consideration for Bottom-up Approach
3.3.18	- Deciding Frequency
3.3.19	- Consideration for Number of Key Risk Indicators
3.3.20	- Thresholds and Limits
3.3.21	- Specialised Thresholds
3.3.22	- Value Proposition of Risk Indicators
3.4	**Analysis**
3.4.1	- Analysis of Loss Related Indicators
3.4.2	- Analysis of Cause Related Indicators
3.4.3	- Analysis of Control Related Indicators
3.4.4	- Risk Monitoring
3.4.5	- Triggers for Escalation
3.4.6	- Managing and Reporting Risk Indicators
3.4.7	- Adding or Changing Indicators
3.4.8	- Taking Action to Resolve Threshold or Limit Breaches
3.4.9	- Comparative Analysis – Joining the Dots
3.4.10	- Overview of KRI Reporting
3.5	**Reporting**
3.5.1	- Level of KRI Reporting
3.5.2	- Reporting to Different Audiences

3.5.3	- Frequency of Reporting
3.5.4	- Data Visualisation
3.6	**Validation**
3.6.1	- Validating Indicators
3.6.2	- Governance, Responsibilities and Assurance
3.7	**Case Studies**
3.7.1	- Case Studies: The Monetary Authority Suspends CHUI Chau Mang For Four Months
3.7.2	- Case Studies: Enforcement Collaboration - Pang Hon Pan Banned For 21 Months
3.8	**Best Practice Guidance**
3.8.1	- Sample Key Risk Indicators (KRI)
3.8.2	- Sample Key Performance Indicators (KPI)
3.8.3	- Sample Key Control Indicators (KCI)
3.8.4	- Sample KRI Reports
3.8.5	- Success Factors in KRI Implementation
Chapter 4: Capital Requirements For Operational Risk	
4.1	**Introduction**
4.1.1	- Introduction
4.1.2	- Concepts and Applications of Accounting Capital, Economic Capital and Risk Weighted Assets
4.1.3	- Difference and Context of Operational Risk Accounting Capital, Economic Capital and Risk Weighted Assets
4.1.4	- Expected Loss and Unexpected Loss in Operational Risk
4.1.5	- Different Tiers Of Capital, LDAC, And The Systemic Risk Buffer Under The Basel Regime
4.2	**Basic Indicator Approach (BIA)**
4.2.1	- Operational Risk Capital Calculation
4.2.2	- Capital Approach
4.2.3	- BCBS Principles
4.2.4	- Position of Various Capital Measurement Approach
4.2.5	- Selection Criteria
4.2.6	- Basic Indicator Approach
4.2.7	- BIA Example 1
4.2.8	- BIA Example 2
4.3	**Standardised Approach (SA)**
4.3.1	- The Standardised Approach
4.3.2	- Advantages of Standardized Approach
4.3.3	- TSA Example 1
4.3.4	- TSA Example 2
4.4	**Alternative Standardised Approach (ASA)**
4.4.1	- Alternative Standardised Approach
4.5	**Advanced Measurement Approach (AMA)**
4.5.1	- Advanced Measurement Approach
4.5.2	- Advanced Measurement Approach Distribution Curve
4.5.3	- AMA Quantitative Stipulations
4.5.4	- AMA Qualitative Stipulations
4.5.5	- Internal Measurement Approach
4.5.6	- Loss Distribution Approach
4.5.7	- Advantages and Disadvantages of LDA
4.5.8	- Standard LDA methods
4.5.9	- Step 1: Modeling Frequency
4.5.10	- Frequency in an LDA Model: Example
4.5.11	- Qualities of the Poisson Distribution
4.5.12	- Step 2: Modeling Severity
4.5.13	- Selecting a Severity Distribution

4.5.14	- The Severity Probability Distribution
4.5.15	- Step 3: Monte Carlo Simulation
4.5.16	- Correlation
4.5.17	- Scenario Analysis Approach to Modeling Operational Risk Capital
4.5.18	- Advantages and Disadvantages of an SA Approach
4.5.19	- Hybrid Approach to Modeling Operational Risk Capital
4.5.20	- Insurance
4.5.21	- Disclosure
4.6	**Revised Standardized Approach (RSA)**
4.6.1	- Revised Standardized Approach
4.6.2	- Methodology of Revised Standardized Approach
4.6.3	- Reduced Risk Management Incentive
4.6.4	- Implications For Banks (Data, systems and processes, business model, capital)
4.6.5	- Business Indicator Component
4.6.6	- Loss Component
4.7	**Case Studies**
4.7.1	- Case Study: Insufficient controls over storage of title deeds of customers
4.8	**Best Practice Guidance**
4.8.1	- Data Comparability Problem
4.8.2	- Changing Level of Operational Risk Capital
4.8.3	- Operational Risk Management Road Map
4.8.4	- Operational Risk Allocation Rules
4.8.5	- Charging Framework (Sample)
Chapter 5: Risk Control Self-Assessment	
5.1	**Introduction**
5.2	**Operational Risk Process and Key Control Analysis**
5.2.1	- Definition of RCSA
5.2.2	- Types and Approaches of RCSA
5.2.3	- General Control Environment Self-Assessment on Minimum Expected Controls
5.2.4	- Characteristics of RCSA
5.2.5	- Benefits of RCSA
5.2.6	- Key Business Identification
5.2.7	- Governance and Responsibilities
5.2.8	- Frequency and Timing
5.2.9	- BCBS Principles
5.3	**Process Risk Mapping and Control**
5.3.1	- Business Process and Process Risk
5.3.2	- Sign off on the Business Process
5.3.3	- Tools on Operational Risk Mapping
5.3.4	- Key Operational Risk Process by Function
5.4	**Business Process Management Tool**
5.4.1	- Business Process Management
5.4.2	- Root Cause Analysis
5.4.3	- Operational Risk Event Types
5.4.4	- Operational Risk Causal Factors
5.4.5	- Risk Assessment Criteria
5.4.6	- Subjective Risk Assessment
5.4.7	- RCSA – Scorecard Approach
5.4.8	- RCSA – Questionnaire Approach
5.4.9	- RCSA Proactive Risk Identification and Management Tool
5.4.10	- Management Results Reporting Tools
5.4.11	- Heat Mapping
5.4.12	- Operational Frequency – Severity Risk Mapping
5.4.13	- RCSA Follow Up

5.4.14	- Advantage and Disadvantage of RCSA
5.5	**Quantification of Potential Exposure**
5.5.1	- Risk (Probability and Impact) Matrix
5.5.2	- Quantification Techniques
5.5.3	- Maximum Potential Exposure
5.6	**Residual Risk Assessment and Treatment**
5.6.1	- Inherent Risk Exposure
5.6.2	- Residual Risk Exposure
5.6.3	- Causes
5.6.4	- Effects
5.6.5	- Action Plan
5.6.6	- Other Elements
5.6.7	- Risk Treatment Strategies
5.6.8	- Operational Risk Action Plan
5.7	**Operational Risk Reporting and Dashboards**
5.7.1	- Reporting RCSA Results
5.7.2	- Reporting Action Planning
5.7.3	- Internal Audit Planning and Reporting
5.8	**Case Studies**
5.8.1	- Case Study: Loss Of Certificates Of Financial Instruments Pledged For Credit Facilities
5.9	**Best Practice Guidance**
5.9.1	- Top-Down and Bottom-Up
5.9.2	- Completing an RCSA: Approaches and Techniques
5.9.3	- Workshop Approach
5.9.4	- Planning
5.9.5	- Attendees
5.9.6	- Structure and Duration of the Workshop
5.9.7	- Facilitation
5.9.8	- Validation
5.9.9	- Questionnaires
5.9.10	- Scope of Questionnaire
5.9.11	- Designing a Questionnaire
5.9.12	- Content of Questionnaire
5.9.13	- Integrating an RCSA into the Operational Risk Management Framework
Chapter 6: Operational Risk Events	
6.1	**Introduction**
6.2	**Different Types of Risk Events**
6.2.1	- Definition of Operational Risk Event
6.2.2	- Identification of Loss Events
6.2.3	- Brainstorming Loss Events
6.2.4	- Defining Loss Events
6.2.5	- Screening Loss Events
6.2.6	- Factors of Review of Loss Events
6.2.7	- Actual Events and Near Misses
6.2.8	- Categorisation of Events
6.2.9	- Governance and Responsibilities
6.2.10	- Basel Consultative Paper – Revisions to Principles for the Sound Management of Operational Risk (PSMOR)
6.3	**Root Cause Analysis**
6.3.1	- Root Cause Analysis
6.3.2	- Fault Tree Analysis
6.3.3	- Ishikawa Cause and Effect Diagram
6.3.4	- Causes of Risk Events
6.3.5	- Control Failures

6.3.6	- Direct And Indirect Impacts
6.3.7	- Financial and Non-Financial Impacts
6.3.8	- Aligning with the Wider Operational Risk Framework
6.3.9	- Operational Risk Causal Factors
6.3.10	- Operational Risk Effect Types
6.4	**Data Collection**
6.4.1	- Data Capture Requirements
6.4.2	- Reasons of Data Collection
6.4.3	- Date and Time of the Event
6.4.4	- Risk Event Type
6.4.5	- Location
6.4.6	- External Data Collection
6.4.7	- Data Collection: Difficulties and Solutions
6.4.8	- Aligning with the Wider Operational Risk Framework
6.5	**Escalation**
6.5.1	- Incident Management and Notification
6.5.2	- Loss Prediction
6.5.3	- Loss Prevention
6.5.4	- Loss Control
6.5.5	- Loss Reduction
6.5.6	- Assumptions, Avoidance and Transference
6.5.7	- Reporting of Operational Risk Events
6.5.8	- Using Operational Risk Event Data
6.5.9	- Using Loss Data to Support Risk Assessments and Monitoring
6.5.10	- Using Loss Data to Support The Risk Appetite and Tolerance Activities
6.5.11	- Using External Data to Benchmark Internal Loss Data
6.5.12	- Using Loss Data to Support the Identification of Emerging Risks
6.5.13	- Insight and Oversight
6.5.14	- Supporting Risk Governance
6.6	**Treatment of Boundary Loss**
6.6.1	- Treatment of Credit Risk Related Operational Risk Events
6.6.2	- Treatment of Market Risk Related Operational Risk Events
6.6.3	- Goodwill Payment
6.6.4	- Single Versus Many Events
6.6.5	- Specific Criteria on Loss Data Identification, Collection and Treatment
6.6.6	- General Criteria on Loss Data Identification, Collection and Treatment
6.6.7	- Lesson Learnt Session
6.7	**Lesson Learnt and Corrective Actions**
6.7.1	- Source Data Documentation
6.7.2	- Training and Awareness
6.7.3	- Review on Other ORM Tools
6.7.4	- External Event Analysis
6.8	**Case Studies**
6.8.1	- Case Study: Use Of Fraudulent Documents And Information For Obtaining Factoring Financing
6.9	**Best Practice Guidance**
6.9.1	- Thematic reviews
6.9.2	- Risk Modelling
6.9.3	- Risk Culture
6.9.4	- Reasons for collecting Operational Risk Event/Loss Data
6.9.5	- Connecting multiple, related events
6.9.6	- Validation of loss estimates
6.9.7	- When to close an event
Chapter 7: Regulatory And Supervisory Frameworks	

7.1	**Introduction**
7.2	**Compliance with Regulatory Standards**
7.2.1	- Recap on Hong Kong Monetary Authority, SA-1: Risk Management Framework; October 2017
7.2.2	- Recap on Hong Kong Monetary Authority, OR-1: Operational Risk Management; July 2022
7.2.3	- Concentration Risk on Outsourcing
7.2.4	- Risk and Impact of Concentration Risk on Outsourcing
7.2.5	- Mitigation and Example of Concentration Risk on Outsourcing
7.3	**Supervisory Approach of Regulators**
7.3.1	- HKMA Risk-based Supervisory Approach
7.3.2	- Relationship with the Prudential Regulator
7.3.3	- Continuous Supervision
7.3.4	- The HKMA's Risk-based Supervisory Methodology
7.3.5	- Risk Assessment Exercise
7.3.6	- Consolidated Supervision
7.3.7	- HKMA Risk Assessment on AI
7.3.8	- Primary prudential obligations of an AI
7.4	**On-Site Examination and Prudential Meetings**
7.4.1	- Preparation for On-site Examinations
7.4.2	- Preparation for Off-site Reviews
7.4.3	- Prudential Meetings
7.5	**Guidelines from The BCBS (10)**
7.5.1	- Recap on Basel Committee: Principles For The Sound Management Of Operational Risk; June 2011
7.5.2	- Recap on Basel Committee: Revisions to the principles for the sound management of operational risk: August 2020
7.5.3	- Basel Committee: Consolidated Basel Framework April 2019
7.5.4	- Revisions To The Principles For The Sound Management Of Operational Risk; March 2021
7.6	**Regulatory Focus**
7.6.1	- Regulatory Focus
7.6.2	- HKMA Work Priorities in 2024
7.6.3	- Key Performance Indicators of Banking
7.7	**Case Studies**
7.7.1	- Case Study: Account takeover using a lost HKID card
7.8	**Best Practice Guidance**
7.8.1	- Regulatory Compliance Toolkit
Chapter 8: Contingency, Business Continuity And Recovery Planning	
8.1	**Introduction**
8.1.1	- Introduction
8.1.2	- Disaster Recovery, Business Continuity and Related Concepts: A Detailed Overview
8.2	**Types of Resilience Risk**
8.2.1	- Definition of Resiliency
8.2.2	- Threats to Financial Resilience
8.2.3	- Interconnects of Financial and Operational Resiliency
8.2.4	- Drivers of Operational Resilience
8.2.5	- Risk, Resilience and Sustainability
8.2.6	- Types of Disasters
8.3	**Resiliency Risk Framework**
8.3.1	- Operational Resilience Framework
8.3.2	- Questions on Operational Resilience
8.3.3	- Common Challenges
8.3.4	- COVID-19 Challenges

8.3.5	- Building Blocks of Operational Resilience
8.3.6	- Approach to Operational Resiliency
8.4	**Effective Tools of Planning, Execution and Testing**
8.4.1	- Business Continuity Planning
8.4.2	- Business Continuity Execution
8.4.3	- Business Continuity Testing and Review
8.4.4	- Business Continuity Insurance
8.5	**Regulatory Requirements**
8.5.1	- Overview of International Regulation and Standard
8.5.2	- Evolution of Regulation on Operational Resiliency (UK)
8.5.3	- Meeting Regulator Expectation
8.5.4	- Regulators Step Up Pressure
8.5.5	- Resilience is a Governance Issue
8.5.6	- IOSCO Principles on Cyber-resilience
8.5.7	- BCBS Consultation on Operational Resiliency, March 2021
8.5.8	- HK Regulators' Position on COVID-19
8.5.9	- HKMA Supervisory Policy Manual (SPM): New module OR-2 on "Operational Resilience" and revised module TM-G-2 on "Business Continuity Planning"
8.5.10	- Effective Incident Management Programme
8.5.11	- HKMA Timeline on Operational Resilience
8.5.12	- BCP and Operational Resilience according to the Hong Kong Monetary Authority
8.5.13	- Business Continuity Planning and Risk Assessment Methodologies
8.5.14	- Incident Response
8.5.15	- Sound Practices for Payment Operations
8.5.16	- Banking Sector's Support for Implementation of Severe Weather Trading
8.6	**Integration into Operational Risk**
8.6.1	- Enterprise Resiliency Office
8.6.2	- Maintaining Financial Resiliency In Post COVID-19
8.6.3	- Integration Operational Resiliency into Operational Risk
8.7	**Case Studies**
8.7.1	- Case Study: Guide to Better Operational Resilience
8.7.2	- Case Study: Disaster – Do not do
8.8	**Best Practice Guidance**
8.8.1	- Take-away on Resiliency Risk Management
8.8.2	- BCP Checklist
8.8.3	- Best Practice of Operational Resilience in Financial Services
Chapter 9: Risk Culture, Awareness And Key Components Of Successful Operational Risk Management Implementation	
9.1	**Introduction**
9.2	**Risk Culture and Awareness**
9.2.1	- Recap on the Importance of Operational Risk Culture
9.2.2	- Performance Metrics of Operational Risk Culture
9.2.3	- How Operational Risk Culture Can Be Improved
9.3	**Importance and Application of Trainings in Operational Risk Management**
9.3.1	- Objectives of Operational Risk Training
9.3.2	- Means of Operational Risk Training
9.3.3	- Contents of Operational Risk Training
9.3.4	- Review and Maintain Operational Risk Training
9.4	**Communication and Engagement Plan of Operational Risk Management in The Workplace**
9.4.1	- Motive: Reduce Routine Losses and Improve Efficiency
9.4.2	- Motive: Reduce the Required Amount of Regulatory Capital
9.4.3	- Motive: Improve Operational Efficiency
9.4.4	- Motive: Overcome Operational Risk Challenges

9.4.5	- Sample Timeline of Communication and Engagement
9.4.6	- Tips for Effective Communication Strategy for Stakeholder Engagement
9.4.7	- Operational Risk Communication
9.4.8	- Operational Risk Engagement
9.4.9	- Winning Over the Firm
9.4.10	- Tactics of Marketing and Communication for Operational Risk
9.4.11	- Overview Of Deliverables By Stakeholders
9.5	**Communication with Senior Management on Operational Risk Topics**
9.5.1	- Communication on Elements of Operational Risk Framework
9.5.2	- Communication on Risk Can Be Aggregated and Presented in Simple and Concise Manner to Senior Management
9.5.3	- Communication on Interpretation of High-Level Operational Risk Results to Draw
9.5.4	- Communication on Meaningful Conclusions and Trends That Will Impact the Organisation
9.5.5	- Communication on Explanation of Operational Risk Measurement Tools and Methodologies in Simple and Concise
9.5.6	- Manner of Communication with All Business Units and Senior Management
9.5.7	- Managing Effective Operational Risk Reporting Process
9.5.8	- Content of Operational Risk Management Information System
9.5.9	- Sample of Operational Risk Report
9.5.10	- Sample of Operational Risk Dashboard
9.5.11	- Objectives of Operational Risk Communication
9.5.12	- Characteristics of Operational Risk Communication
9.5.13	- Topics of Operational Risk Communication (Examples)
9.5.14	- Key Points to Convey in Operational Risk Communication
9.5.15	- Usability of Operational Risk Communication
9.5.16	- Guideline of Delivery of Operational Risk Communication
9.5.17	- Timeliness of Communication
9.6	**Oversight, Monitoring and Understanding of Relevant Operational Risk Management Processes Taken Up by Subject Matter Experts**
9.6.1	- Engagement Model between Operational Risk and Internal Audit
9.6.2	- Engagement Model between Operational Risk and Compliance
9.6.3	- Engagement Model between Operational Risk and Business Continuity
9.6.4	- Engagement Model between Operational Risk and Other Subject Matter Experts
9.6.5	- Input of Subject Matter Experts on Various Risk Areas
9.6.6	- Key Function of Subject Matter Experts – Technology Risk (Illustration)
9.6.7	- Key Function of Subject Matter Experts – Conduct Risk (Illustration)
9.6.8	- Key Function of Subject Matter Experts – Data Privacy Officer (Illustration)
9.6.9	- Key Function of Subject Matter Experts – Financial Crime (Illustration)
9.6.10	- Key Function of Subject Matter Experts – Vendor Risk Management (Illustration)
9.7	**Case Studies**
9.7.1	- Case Study: Enforcement action against Société Générale by the SFC following the investigation of the HKMA
9.8	**Best Practice Guidance**
9.8.1	- Example Reporting Matrix – Content, Recipient And Frequency
9.8.2	- Top 5 Successful Factors in ORM Reporting and Why They Are Important
Chapter 10: Operational Risks Related To The Key Areas For Future Banking	
10.1	**Introduction**
10.2	**Green and Sustainable Banking**
10.2.1	- Current Landscape
10.2.2	- Climate Risk Concept
10.2.3	- Types of Climate Risks
10.2.4	- Climate Risk Impact
10.2.5	- Physical and Transition Risk
10.2.6	- Key Climate Related Risk for Financial Institutions

10.2.7	- Managing Climate Risk
10.2.8	- Climate Risk and Opportunities
10.2.9	- Task Force on Climate Related Financial Disclosure (TCFD)
10.2.10	- TCFD Recommendations
10.2.11	- TCFD Supplement Guidance
10.2.12	- How Banks Addressing Climate Risk
10.2.13	- TCFD/ISSB Key Implementation Challenges
10.2.14	- Typology of Physical Risk
10.2.15	- From Physical Risk to Financial Stability Risk
10.2.16	- Typology of Transition Risk
10.2.17	- From Transition Risk to Financial Stability Risk
10.2.18	- Climate Financial Risk Assessment
10.2.19	- Example of Climate Risk Impact on Bank
10.2.20	- How Financial Firms Addressing Climate Risk
10.2.21	- Climate Risk Framework
10.2.22	- HKMA Climate Risk Initiative
10.2.22	- Four Biodiversity-related Financial Risks
10.2.23	- Operational Risk Assessment
10.2.24	- Climate Risk Stress Testing
10.2.25	- Operational Risk Scenarios (Example)
10.2.26	- Incorporating Climate Risk into Enterprise Risk
10.2.27	- HKMA Climate Risk Framework
10.2.28	- Governance: Key Takeaways
10.2.29	- Strategy: Key Takeaways
10.2.30	- Risk Management: Key Takeaways
10.2.31	- Disclosure: Key Takeaways
10.2.32	- HKMA Publishes Report On First Climate Risk Stress Test of The Hong Kong Banking Sector
10.2.33	- HKMA Guidelines for Banking Sector Climate Risk Stress Test
10.2.34	- Hong Kong Green Taxonomy
10.2.35	- HK's Green and Sustainable Finance Strategy
10.2.36	- Cross-agency Steering Group Announces Priorities To Further Strengthen Hong Kong's Sustainable Finance Ecosystem
10.3	**Digital Banking Services**
10.3.1	- Journey of Intelligent Process Automation
10.3.2	- Adversarial Risk
10.3.3	- Risk Assessment Framework
10.3.4	- Technology Risk Assessment Framework
10.3.5	- Third Party Risk Assessment Framework
10.3.6	- Recognition of Risk and Control
10.3.7	- Proactive Risk and Control Consciousness
10.3.8	- Call to Action
10.3.9	- Emerging Risk in Fintech
10.3.10	- Risk Questions to Answer
10.3.11	- Operational Risk in Retail Payments and Digital Wallets
10.3.12	- Operational Risk in Fintech Credit
10.3.13	- Operational Risk in Robo-advisors
10.3.14	- Operational Risk in DLT-based Wholesale Payment Systems
10.3.15	- Operational Risk in Private Digital Currencies
10.3.16	- Operational Risk in AI and Machine Learning
10.3.17	- Overview of Digital Banking
10.3.18	- Trends of Digital Banking
10.3.19	- Risks and Mitigants of Digital Banking
10.3.20	- Prospect and Outlook of Digital Banking

10.3.21	- Promotion of Mobile Point-of-Sale (POS) Terminals
10.4	**Case Studies**
10.4.1	- Case Study: The HKMA suspends Leung Wai Yu for three months
10.5	**Best Practice Guidance**
10.5.1	- HKMA "White Paper on Green and Sustainable Banking"
10.5.2	- HKMA Develops Two-year Roadmap To Promote RegTech Adoption
10.5.3	- HKMA FinTech 2025
Chapter 11: The Future and Challenges Of Operational Risk Management	
11.1	**Introduction**
11.2	**Competence Development**
11.2.1	- ORM Officer Professional Standard Summary of Core Competencies
11.2.2	- HK SFC Managers-In-Charge of Core Functions (MIC)
11.2.3	- HKMA Enhanced Competence Framework for Banking Practitioners
11.2.4	- Strengthening Individual Accountability
11.2.5	- Competencies of an Operational Risk Professional in Hong Kong
11.3	**Emerging and Proactive Risk Management**
11.3.1	- Performing Environmental Scanning
11.3.2	- Proactive ORM Monitoring
11.3.3	- Forces Driving Complexity, Increasing Risk
11.3.4	- Identification of Emerging Risks and Opportunities
11.3.5	- Use of Operational Risk in Decision Making
11.3.6	- Early Warning Signal
11.3.7	- Develop Scenarios
11.3.8	- Generate Options and Strategy
11.3.9	- Implement Strategy
11.3.10	- Review Risk Development
11.3.11	- Effective Lines of Defense
11.3.12	- Predictive Risk Intelligence
11.3.13	- Embedding Operational Risk into Business
11.3.14	- Overview of Deliverables by Stakeholders
11.4	**Deployment of Artificial Intelligence**
11.4.1	- Key Trends in Artificial Intelligence
11.4.2	- Application of Technology in the Financial and Non-financial Risk Management
11.4.3	- Priority of RegTech and RiskTech
11.4.4	- GARP Survey on AI/RPA
11.4.5	- AI Adoption in Risk Management
11.4.6	- Risk Managers in Assessing AI Adoption or Non-adoption Risk
11.4.7	- Empower Risk and Compliance
11.4.8	- Trade Lifecycle Enabled by AI
11.4.9	- Digitisation of Risk Management
11.4.10	- CCAR and Stress Testing
11.4.11	- Risks and Opportunities: Questions on AI
11.4.12	- Using AI/Machine Learning in Operational Risk Management
11.4.13	- Key Points on AI Development Path
11.5	**Challenges and Solutions**
11.5.1	- Intrinsic Difficulties of Operational Risk
11.5.2	- Overcoming The Operational Risk Challenges
11.5.3	- Opportunity Window
11.5.4	- Potential Pitfalls And Workable Solutions
11.5.5	- Integrating ORM Framework
11.5.6	- Engaging the Right People
11.5.7	- Adding Value
11.5.8	- Action Roadmap – Things That Are Usually Overlooked!
	-

11.5.9	- What Does Success Look Like
11.5.10	- Key Elements to Embed Operational Risk
11.5.11	- Operational Risk Deliverables
11.5.12	- The Future of Operational Risk
11.5.13	- Defining Next-generation Operational-risk Management
11.5.14	- Develop Second-line Oversight To Ensure Operational Excellence And Business-process Resiliency
11.5.15	- Transform Risk Detection With Data And Real-time Analytics
11.5.16	- Develop Talent And The Tools To Manage Specialized Risk Types
11.5.17	- Bank Employees Drive Corporate Performance But Are Also A Potential Source Of Operational Risk
11.5.18	- Manage Human-factor Risks
11.5.19	- Targeted Analytics Tools
11.5.20	- Operational Risk Maturity Model
11.6	**Case Studies**
11.6.1	- Case Study: The Monetary Authority Suspends Chu Lai Kwan for Breaching the Code of Conduct and Internal Policy of Her Employer
11.7	**Best Practice Guidance**
11.7.1	- AI/Machine Learning in Operational Risk Use Cases
11.7.2	- Overcome ORM Challenges Toolkit
Chapter 12: Integrated Case Studies And Best Practices	
12.1	**Introduction**
12.2	**Integrated Case Studies**
12.2.1	- Operational Risk Lessons from the OCC's Citibank Fine
12.2.2	- Punjab National Bank Letter of Commitment Fraud
12.2.3	- Aussie banks pay for underpaying staff
12.2.4	- Citibank Payment Error
12.3	**Best Practice Guidance**
12.3.1	- Interbank payment weaknesses
12.3.2	- Swiss tax evasion
12.3.3	- Data breaches top $2bn since 2012

D. 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. (2025). Advanced Operational Risk Management.

Supplementary Readings

1. Basel Committee. (2021). Revisions To The Principles For The Sound Management Of Operational Risk.
2. Basel Committee. (2020). The Basel Framework: Frequently Asked Questions.
3. Basel Committee. (2021). Principles For Operational Resilience.
4. Basel Committee. (2019). Launch Of The Consolidated Basel Framework.
5. Basel Committee. (2018). Sound Practices: Implications Of Fintech Developments For Banks

And Bank Supervisors.
6. Basel Committee. (2017). Basel III: Finalising Post-Crisis Reforms.
7. Hong Kong Monetary Authority. (2019). TM-E-1: Risk Management of E-Banking.
8. Hong Kong Monetary Authority. (2017). IC-1: Risk Management Framework.
9. Hong Kong Monetary Authority. (2022). OR-1: Operational Risk Management in Supervisory Policy Manual.
10. Hong Kong Monetary Authority. (2022). TM-G-2: Business Continuity Planning.
11. Hong Kong Monetary Authority. Operational Incidents Watch.
12. Hong Kong Monetary Authority. (2020). Report on Review of Self-assessments on Bank Culture.
13. Hong Kong Monetary Authority. (2018). Supervision for Bank Culture.
14. Hong Kong Monetary Authority. (2017). Bank Culture Reform.

Further Readings

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

7. Training Application

7.1 Training Schedule

For the latest information about the training application period and class schedules, pleaserefer to Training Schedule on HKIB website.

7.2 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

7.3 Training Application

Applicants can submit the application via MyHKIB. Attention should be paid to the application deadline, or a late entry fee will be charged.

Application Requirements:

- The information provided for the training enrolment must be true and clear.
- Inaccurate or incomplete applications may not be accepted even if the applicant has paidthe training fee.
- HKIB reserves the right to reject late applications and/or any applications deemed inappropriate. Once HKIB has received your application, NO alterations to the training arrangement are allowed.
- HKIB reserves the right to change training dates and application deadlines at any time.

7.4 Training Fee and Payment

Module	***Training Fee per module***
1	HKD4,400 *
2	HKD4,400 *
3	HKD4,400 #

4	HKD7,000 #

* *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 HKD600 (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 HKD600 (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 credit card.
  (b) By Alipay.
  (c) By WeChat Pay.
- Application without successful payment will **NOT** be 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 payments.
- An email of training confirmation will be sent to applicants at least **five 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.
- HKIB student members can enjoy 25% off training fee discount.

8. Examination Application and Regulations

8.1 Examination Mode and Format

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

Module	1/ 2	3
Examination Mode	Paper-based Examination	
Examination Duration	1.5 Hours per Module	2.5 Hours per Module
Question Type	Multiple-choice Type Questions (MCQs)	
No. of Questions	50 MCQs per Module	80 MCQs per Module
Pass Mark	70%	
Grading	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:

Module	4	
Examination Mode	Paper-based Examination	
Examination Duration	3 Hours	
Question Type	Multiple-choice Type Questions (MCQs) & EssayType Questions	
No. of Questions	50 MCQs with 2 out of 3 essay type questions	
Pass Mark	60%	
Grading	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

8.2 Examination Timetable

- For latest information about the examination application period and examination dates,please refer to Examination Schedule on HKIB website.

8.3 Examination Approaches

There are two examination approaches available and candidates may choose either one which is best for them.

- Face-to-face Examination: Traditional face-to-face examinations will be conducted at designated venues arranged by HKIB. Candidates are required to take examinations at specific locations allocated to them accordingly.
- "Remote Exam": As an alternative to the traditional face-to-face examination, HKIB had introduced an innovative initiative, "Remote Exam", allowing candidates to take examinations from their homes or workplaces with own computer equipment and internet access. "Remote Exam" offers greater flexibility in terms of location and time saving on travelling for our candidates without jeopardising the quality standard of assessment.

  Measures will be taken to align the same standard of fairness and effectiveness as that of the traditional face-to-face examination. A two device-approach will be adopted with one computer, either desktop or laptop, to access the "Remote Exam" platform for the examination and a mobile device, either smartphone or tablet, for invigilation and monitoring. Authentication of identity and real-time virtual invigilation will be conducted hassle-free with an automatic remote system to ensure the highest degree of integrity and data security.

  To ensure smooth examination operations, candidates opting "Remote Exam" are required to participate in the "Rehearsal Practice Examination" to be held by HKIB before eligible to attend the formal examination. This arrangement will facilitate the candidates to get better preparation and understanding on the logistic arrangement of the "Remote Exam".

8.4 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 via MyHKIB. Attention should be paid to the application deadline or a late entry fee will be charged. The information provided on the application form must be true and clear.
- 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.
- 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 your application, NO alterations to the examinations and examination arrangements are allowed.
- HKIB reserves the right to change examination dates and application deadlines at any time.

8.5 Examination Fee and Payment

Module	*Examination Fee per module* #
1 – 2	HKD600
3	HKD1,300
4	HKD1,600

HKIB student members can enjoy 50% off examination fee discount.

- Applicants should pay the examination fee as follows:

  (d) By credit card.

  (e) By Alipay.

  (f) By WeChat Pay.

- Application without successful payment will **NOT** be 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.
- HKIB reserves the right to adjust the examination, study guide and/or administration surcharge fees (if applicable), at any time.

8.6 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.
- For candidates attending "Remote Exam", details regarding the prerequisite "Rehearsal Practice Examination" will also be attached.

8.7 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 one 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.

8.8 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.

8.9 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.

8.10 Examination Results

Examination Results Announcements

	*Examinations **before** March 2026*	*Examinations **after** March 2026*
Email notification on results	Yes	
Examinations with multiple-choice type questions ONLY	Results will be released within **four weeks** after the examination date	
Examinations with the presence of essay-type questions	Result will be released around **eight weeks** after the examination date of the last module of the exam diet	
Platform for result checking	HKIB online platform (valid for one month only after the result release date)	MyHKIB
Official examination result slip	Receive within two weeks after the result release date through HKIB online platform	MyHKIB

- 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.

Examination Results Review

- Candidates may request rechecking or remarking of their examination scripts, within one month of the issue of examination results by submitting an official Examination Result Appeal Form via HKIB website.
- Rechecking fee of HKD500 per module is only applicable for multiple choice examinations and this fee covers the re-checking for technical errors only such as incorrect mark entries for multiple-choice answer sheets. Remarking fee of HKD1,700 per module is only applied to other types of examination.

8.11 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 examinationsand candidates are required to abide by the policies of HKIB. Calculators are inspectedprior to the start of the exam. They must remain on your desk in full view and proctorscontinue to inspect calculators throughout the administration of the examination. Possession or use of an unauthorised calculator at the test centre results in the voidingof your examination results and may lead to the suspension or termination of yourcandidacy in HKIB Programme. Failure by the proctors to detect an unauthorisedcalculator prior to the start of the examination, or your use of an unauthorised calculatorat any time during the examination, does not imply that the calculator is an approvedmodel 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.

8.12 Examination Misconduct Handling

This section sets out the standards of conduct expected from candidates during HKIB examinations and the procedures for handling alleged misconduct.

1. Any infringement of these guidelines may result in disciplinary action, including disqualification.
2. Candidates who contravene the proper conduct of the examination will be warned by the invigilator or, in serious cases, expelled from the examination room. In such instances, a report will be submitted to HKIB for consideration of disciplinary action. Disciplinary measures may include, but are not limited to, disqualification of the candidate.
3. Candidates are strictly prohibited from communicating with other candidates during the examination. They must also refrain from contacting any third parties outside the examination room through any electronic device. The invigilator reserves the right to remove any candidate whose behaviour disrupts the proper conduct of the examination. Any candidate found attempting to copy from another candidate's script or conduct any other form of plagiarism or collusion will be disqualified.
4. Examples of misconduct during examination include:
   a. Improper communication or contact with other candidates
   b. Use of unauthorised electronic or communication devices
   c. Sharing, photographing, or otherwise capturing examination content
   d. Suspicious or disruptive behaviour (e.g., repeated eye movements suggesting copying)
   e. Possession of prohibited materials
   f. Causing unnecessary disturbance in the examination room
   g. Engaging in cheating, contract cheating or collusion
5. In determining whether misconduct has occurred, HKIB may consider the candidate's possible motive, any attempt to engage in misconduct, or any conduct that constitutes misconduct.
6. In the event of suspected misconduct by examination candidates, HKIB will implement a thorough and robust investigation process. If it is determined that misconduct has occurred, HKIB will notify the relevant candidate in writing.
7. As part of the appeal process for HKIB's decision, the candidate will have the opportunity to submit a written representation, including any mitigating factors, within 30 calendar days after providing intention notification to HKIB, providing any additional information or documentation as appropriate.

If deemed necessary, HKIB may convene a disciplinary hearing panel, comprising members of HKIB Committees and attended by the candidate, to determine a final decision on the matter. During the hearing, the candidate will be given the opportunity to present additional information verbally. The candidate will receive the written final decision within 5 business days after the disciplinary hearing panel hearing.

8. Candidate behaviour considered to constitute misconduct during the examination will be classified into three levels of severity:

    Level 1: Individual dishonest behaviour without question leakage

    Examples:

    i. Continuing to write after the "time's up" announcement
    ii. Attempting to copy from another candidate

    Level 2: Individual dishonest behaviour with question leakage

    Examples:

    i. Attempting to communicate with a third party during the exam
    ii. Taking photos or recordings of the question paper

    Level 3: Group dishonest behaviour with question leakage

    Example:

    i. Sharing or coordinating answers among a group of candidates who are in the examination room

9. The reference starting points for penalties arising from candidate misconduct, corresponding to the three levels of severity, are as follows:
    a. Level 1: Suspension from enrolling in HKIB Professional Qualifications Examinations for a period of 1 year; together with mandatory participation in a "remediation programme" as specified by HKIB.
    b. Level 2: Suspension from enrolling in HKIB Professional Qualifications Examinations for a period of 3 years; together with mandatory participation in a "remediation programme" as specified by HKIB.
    c. Level 3: Suspension from enrolling in HKIB Professional Qualifications Examinations, and exclusion from admission as a member and/or as a professional qualification holder, for a period of five years; together with mandatory participation in a "remediation programme" as specified by the HKIB.
10. The remediation programme will require mandatory participation in designated training courses provided by HKIB, focusing on professional ethics and compliance.
11. The decision of the disciplinary hearing panel is final.
12. HKIB will record all misconduct cases in the candidate's personal records maintained by it.

9. Certification Application and Renewal Process

9.1 Certification Application

Relevant Practitioners who have completed Modules 1 to 3 of the ECF-ORM (Core Level) Programme and obtained a pass in the relevant examinations, may apply for the certification AORP with HKIB professional membership.

Relevant Practitioners who have completed Modules 4 of the ECF-ORM (Professional Level) Programme and obtained a pass in the relevant examination plus at least 5 years of relevant work experience as specified in Annex 1 of the HKMA Guide to Enhanced Competency Framework on Operational Risk Management, may apply for the certification CORP with HKIB professional membership.

Applicants are required to submit a completed Certification Application Form 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.

Certification holders are registered as Certified Individuals and included in the public register on HKIB website. Upon successful application for the above Certification(s), professional membership is also granted by HKIB.

9.2 Certification Renewal

Certification of AORP and CORP are subject to annual renewal by HKIB.

PQ holders are required to comply with the annual Continuing Professional Development (CPD) Scheme in order to renew their Certification.

For both Core Level and Professional Level qualifications, the requirement is a minimum of 12 verifiable CPD hours, of which at least 6 hours should be earned from activities related to the topics of compliance, legal and regulatory requirements, risk management and ethics.

The remaining hours should be on training topics related to banking and finance or the job function. Examples of appropriate training topics include:

a) Compliance, code of conduct, professional ethics or risk management;
b) Banking and financial knowledge;
c) Economics;
d) Accounting;

e) Legal principles;
f) Business and people management;
g) Language and information technology; and
h) Subject areas covered in HKIB's professional examinations.

PQ holders are required to renew their certification registration annually by 31 December. Renewal email will be sent to members before renewal deadline. PQ holders who do not pay the certification renewal fee on or before 31 January of each calendar year are treated as Default Members.

9.3 Certification Fee, Certification Renewal Fee and Payment

- The application fee for Certification in various categories are as follows: (Valid until 31 December 2026)

Certification	First year certification - Non-HKIB Member: HKD2,230 - Current HKIB Ordinary Member (a) Complimentary: HKD2,230 / 970* - Current HKIB Professional Member: Waived
Certification Renewal	Annual Certification Renewal - Current HKIB Professional Member: HKD2,230 - Reinstatement fee for default member: HKD2,000

* Members who have paid the HKD1,260 Ordinary Membership fee for the current membership year are required to pay only the difference of HKD970 to complete their certification application.

- Applicants should pay the Certification Fee and Certification Renewal Fee:
  (a) By Employer.
  (b) By credit card. Please provide your credit card information on the application form**.**
  (c) By FPS payment. Please provide your FPS payment receipt.
- 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.

9.4 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 [1] of documentary confirmation, e.g. Hong Kong Identity Card, birth certificate, statutory declaration, etc.

Certification 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. Certification 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 certification holders made with respect to applications, and applicants may be subject to disciplinary actions for any misrepresentation (whether fraudulent and otherwise) in their applications.

9.5 Membership Reinstatement

Professional Members who have not paid the certification renewal fee when due shall be considered as default members and are not entitled to use any HKIB Professional Qualification and neither call themselves members of the Institute.

Default members who reinstate their membership with HKIB are required to pay the current year's certification renewal fee plus a reinstatement fee. Once the membership is reinstated, the member's examination record, if any, is reactivated.

[1] 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 recognised certified public accountant / lawyer / banker / notary public; or
- Hong Kong Institute of Chartered Secretaries (HKICS) member.
- The certifier must sign and date the copy document (printing his/her name clearly in capital letters underneath) and clearly indicate his/her position on it. The certifier must state that it is a true copy of the original (or words to similar effect).

10. Exemption Application and Regulations

10.1 Modular Exemption Requirements

Exemption for specific modules of the training programme will be granted for practitioners who have passed any of the following training / professional programme(s):

Module	Eligibility for exemption
Module 1	• Certification in Risk Management Assurance of the Institute of Internal Auditors; or • Bachelor's or higher degree in law; or • Professional Ethics and Compliance module under the Advanced Diplomafor Certified Banker (Stage I) of HKIB; or • Certified Professional Risk Manager of the Asia Risk Management Institute (ARIMI); or • Certified Public Accountant of the Hong Kong Institute of Certified Public Accountants (HKICPA); • Full member of Association of Chartered Certified Accountants (ACCA); or 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)
Module 3	• Operational Risk Manager Certificate of the Professional Risk Managers' International Association (PRMIA); or • Professional Risk Manager of the PRMIA; or • 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.

10.2 Modular Exemption Application

- Candidate with relevant qualifications may apply for modular exemption on the above modules of the ECF-ORM Core Level.
- 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

  Note: Candidates are required to submit the exemption form ONLY if they attended the training and completed the examination offered by HKIB.
- 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 60 days 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, learners/candidates should pay attention to announcement made by the Hong Kong Observatory about weather conditions. They could also visit HKIB website for its announcements. For the respective individuals, they will be notified by SMS message about the latest arrangements.

Bad weather – Typhoon signal No. 8 or above, or the black rainstorm signal, or "extreme conditions" is hoisted.

For On-site Training

Signal in force	Bad Weather Arrangement
At or after 7am	Session starts from 9:00am to 2:00pm will be switched to virtual training class/event whenever possible.
At or after 12:00noon	Session starts from 2:00pm to 6:00pm will be switched to virtual training class/event whenever possible.
At or after 4:00pm	Session starts from 6:00pm to 10:00pm will be switched to virtual training class/event whenever possible.

For On-site Examination

Signal in force	Bad Weather Arrangement
At or after 7am	Session starts from 9:00am to 2:00pm will be rescheduled.
At or after 12:00noon	Session starts from 2:00pm to 6:00pm will be rescheduled.
At or after 4:00pm	Session starts from 6:00pm to 10:00pm will be rescheduled.

For Virtual Training / Remote Examination

Signal in force	Bad Weather Arrangement
At or after 7am	Session starts from 9:00am to 2:00pm will be continued as per schedule whenever possible.
At or after 12:00noon	Session starts from 2:00pm to 6:00pm will be continued as per schedule whenever possible.
At or after 4:00pm	Session starts from 6:00pm to 10:00pm will be continued as per schedule whenever possible.

11.2 Privacy Policy Statement

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 in writing to HKIB by using HKIB's email address of cs@hkib.org.

Candidates are advised to read the Privacy Policy Statement at HKIB website 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.

11.3 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 / Feedback

Tel.: (852) 2153 7800

Email: cs@hkib.org

Office Service Hours

Monday – Friday: 09:00 - 18:00 (except public holidays)