HONG KONG MONETARY AUTHORITY
香 港 金 融 管 理 局

Our Ref: B9/166C

18 December 2020

The Chief Executive
All Authorized Institutions

Dear Sir/Madam,

Enhanced Competency Framework on Operational Risk Management

I am writing to announce the launch of the Enhanced Competency Framework on Operational Risk Management (ECF-ORM).

The ECF-ORM is a collaborative effort of the HKMA, the Hong Kong Institute of Bankers (HKIB) and the banking sector in establishing a set of common and transparent competency standards for raising the professional competence of relevant practitioners working in the operational risk management function of authorized institutions (AIs). This framework will facilitate talent development and help enhance the professional competencies of bank staff engaged in operational risk management.

Details of the ECF-ORM, including its scope of application, competency standards, qualification structure, certification and grandfathering arrangements, and continuing professional development (CPD) requirements are set out in the Guide attached to this letter.

As the Supervisory Policy Manual module CG-6 "Competence and Ethical Behaviour" emphasises the importance of ensuring continuing competence of staff members, AIs are encouraged to adopt the ECF-ORM as part of their overall efforts in supporting relevant employees' on-going professional development. The HKMA expects AIs to adopt appropriate measures to monitor and maintain the competence levels of their operational risk management staff.

Apart from supporting their staff to attend trainings and examinations that meet the ECF certification, AIs are also advised to keep proper records of the relevant training and qualification of their staff and to provide them with necessary assistance in their applications for grandfathering and certification, and fulfilment of CPD training under the ECF-ORM.

The HKIB is the administrator of the ECF-ORM, whose major role includes handling certification and grandfathering applications, administering the examinations and CPD requirements, and maintaining a public register of qualified certification holders. AIs may direct any enquiries regarding certification, grandfathering, training and other related matters to Mr Wallace Hui at 2190 7088 or Mr Henry Lee at 2190 7028 / 2153 7800 of the HKIB.

Meanwhile, if there are any enquiries concerning this circular, please feel free to contact Ms Ivy Yong at 2878 8495 or Miss Rita Kong at 2878 8303.

Yours faithfully,

Daryl Ho
Executive Director (Banking Policy)

Encl

cc: FSTB (Attn: Ms Eureka Cheung)
HKIB (Attn: Ms Carrie Leung)

Guide to

Enhanced Competency Framework

on Operational Risk Management

Hong Kong Monetary Authority

18 December 2020

Table of Contents

1. Introduction

1.1 The Enhanced Competency Framework (ECF) is a collaborative effort of the Hong Kong Monetary Authority (HKMA) with relevant professional bodies and the banking sector in establishing a set of common and transparent competency standards for different professional areas which are central to the safety and soundness of authorized institutions (AIs) and where talent shortages are more apparent. The development of a set of competency standards will enable more effective training for new entrants and support the ongoing professional development of existing practitioners in the banking industry. This will contribute to maintaining the competitiveness of Hong Kong as an international financial centre. To date, the HKMA has launched six ECF modules, namely private wealth management, anti-money laundering and counter-financing of terrorism (AML/CFT), cybersecurity, treasury management, retail wealth management and credit risk management.

1.2 Operational risk management is vital in preventing, managing, and assessing the risk of direct or indirect loss resulting from inadequate or failed internal processes, people, systems or external events. In recent years, the importance of operational risk management is exemplified by the greater variety and severity of business disruptions, frauds or other operational incidents. Such operational events require organisations to be nimble, responsive, and adapt to rapidly evolving market conditions. Against such a background, there is a clear demand for banking practitioners to be equipped with the required skills and knowledge to properly manage operational risk and to facilitate the development of the required policies, procedures, and controls accordingly.

1.3 The ECF-ORM is aimed at equipping banking practitioners with the technical skills and professional knowledge required in the day-to-day activities of the operational risk management function of an AI.

2. Objectives

2.1 The ECF-ORM is a non-statutory framework which sets out the common and core competences required of operational risk management practitioners in Hong Kong's banking industry. The objectives of the ECF-ORM are twofold:

(a) to develop a sustainable talent pool of operational risk management practitioners for the banking industry; and

(b) to raise the professional competence of existing operational risk management practitioners in the banking industry.

2.2 Although the ECF-ORM is not a mandatory licensing regime, AIs are encouraged to adopt it for purposes including but not limited to:

(a) using the ECF-ORM as a benchmark to determine the level of competence required and assess the ongoing competence of relevant employees;

(b) supporting relevant employees to attend training programmes and examinations that meet the ECF-ORM benchmark;

(c) supporting the continuing professional development (CPD) of relevant employees; and

(d) promoting the ECF-ORM as an industry-recognised qualification, including for recruitment purposes.

2.3 The ECF-ORM is designed to cover practitioners who are in charge of managing operational risks within an AI in Hong Kong. The structured competency framework would enable relevant practitioners to develop the required technical skills and professional knowledge for managing operational risks within an AI.

2.4 The ECF-ORM comprises the following two elements:

(a) Competency standards
These standards are derived from the job skills and competencies required for 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 in the operational risk management function of an AI.

(b) Qualification standards

These standards are derived from prevailing market practices in qualifying operational risk management practitioners, including certifications recognised by AIs in Hong Kong, grandfathering and CPD for the required qualifications.

3. Scope of application

3.1 Sound operational risk management is a reflection of the effectiveness of the board and senior management of an AI in administering its portfolio of products, activities, processes, and systems[1]. Operational risk management is performed by both the first and second lines of defence of an AI. Within the operational risk management process, relevant practitioners' responsibilities can typically be segregated into the five components in Table 1 below. Depending on the organisational structure and the assignment of roles and responsibilities within an AI, the activities below may be the responsibility of the first line of defence, the second line of defence, or even both the first and second lines of defence. A strong risk culture and good communication among the first and second lines of defence for operational risk management and the third line of defence (i.e. internal audit) are important characteristics of good operational risk governance.

Table 1 – Operational risk management process

<table>
<tr><th colspan="4">(i) Risk Governance Framework</th></tr>
<tr><td colspan="4">• Promote a culture of "governance, risk and control" throughout the AI.
• Initiate the development of risk governance, policies, internal controls and processes with the overall objective of risk management, control awareness and enhancement to operational efficiency.
• Assist in identifying compliance and internal control issues and monitor the ongoing progress of improvement actions.</td></tr>
<tr><th>(ii) Risk identification and assessment</th><th>(iii) Risk monitoring and reporting</th><th>(iv) Risk control and mitigation</th><th>(v) Business resiliency and continuity planning</th></tr>
<tr><td>• Identify and assess the operational risks inherent in all existing or new material products,</td><td>• Monitor operational risk profiles and material exposures to losses on an on-</td><td>• Keep properly documented policies, processes and procedures to manage and/or mitigate</td><td>• Establish business resiliency and continuity plans to ensure operation on an ongoing basis</td></tr>
</table>

[1] Basel Committee on Banking Supervision, *Principles for the Sound Management of Operational Risk*, June 2011

activities, processes and systems, based on the AI’s own defined operational risk management strategy and risk appetite. • Perform operational risk and control self-assessments, including mapping of key risks and identification and quantification of risk indicators. • Perform scenario analysis/assessment and stress testing to identify potential operational losses, followed by subsequent analysis based on event type.	going basis. • Perform both qualitative and quantitative monitoring and reporting of the AI’s exposure to all types of operational risk, including trend analysis of risk profiles. • Report outcomes from operational risk assessments to senior management. Assess the quality and appropriateness of remedial actions identified. • Monitor and review the limits of operational risk regulatory and economic capital. • Ensure that adequate monitoring and reporting controls are in place to identify and address operational risks. • Ensure reporting and escalation of operational risk events/incidents occurs in a timely manner, and that periodic monitoring of issue resolution occurs to ensure timely resolution.	operational risks. • Have a system in place for ensuring compliance with internal policies concerning the AI’s operational risk management system. • Assess operational risk control effectiveness, including control design and execution. • Maintain operational risk management system and quality of operational loss data. • Initiate, manage, and execute governance and controls related initiatives/tasks to ensure full compliance of operational risk policies and regulatory requirements. Ensure these tasks are completed in a timely manner.	and limit losses in the event of severe business disruption. • Perform testing of the plans regularly and update the plans regularly to incorporate changes to operations, business requirements, and risks to ensure an efficient response is provided to business interruption events.

3.2 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.

3.3 Specifically, it is aimed at "Relevant Practitioners" (RPs) located in the Hong Kong office of an AI who perform the operational risk management job roles listed in Table 2 below.

Table 2 – Job roles of the ECF-ORM

	Role 1 – Operational Risk Management (i.e. staff in charge of managing operational risks in the second line of defence)	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)
Responsibilities	• Assist management in meeting their responsibility for understanding, monitoring and managing operational risks; • Develop and ensure consistent application of operational risk policies, processes, and procedures throughout the AI; • Ensure that the first line of defence activities are compliant with such policies through conformance testing; • Perform and assess stress testing and related scenario analysis; and • Provide training to and advise the business units on operational risk management issues.	• 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; • Escalate operational risk events to senior management and operational risk management staff in the second line of defence, as required; • 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; and • Develop risk indicators, determine escalation triggers and provide management reports.

3.4 The definition of RPs has taken into account differences among AIs in how operational risk management practitioners are assigned within different organisational structures. Functional roles rather than the functional titles of staff members should be essential in considering whether the definition of RPs is met. To facilitate the determination of whether a staff member falls under the scope of RPs, please refer to the key tasks outlined in Annex 1.

3.5 It should be noted that the ECF-ORM is not intended to cover staff members performing the following functions:

a) Practitioners performing cybersecurity roles within an AI as they are subject to the ECF-Cybersecurity. Please refer to the HKMA's Guide to ECF on Cybersecurity for details of these roles.

b) Practitioners currently performing corporate and administrative services within an AI, including (but not limited to) human resources, IT, corporate security and marketing.

c) Staff in the operational risk management functions within an AI who are performing solely clerical and administrative duties or other incidental functions.

d) Staff in the legal/compliance or the internal audit function of an AI (it should be noted that Core Level and Professional Level qualifications and/or grandfathering can be achieved through internal audit experience related to operational risk management and controls within an AI. Please refer to sections 5.1 and 7.1 below for more details).

e) Senior management or relevant risk committee members (e.g. operational risk committee members) other than the manager or person-in-charge of the operational risk management department.

3.6 For the avoidance of doubt, a staff member is not required to work full time in the operational risk management function or perform all of the roles specified in the job description in order to be classified as a RP. AIs are expected to adopt a principles-based approach when determining whether a staff member with multiple job roles falls within the definition of RPs for the ECF-ORM by assessing the significance of the operational risk management role performed by the staff member. AIs are expected to justify their decisions made in this regard.

4. Competency standards

4.1 Competency standards are set at two levels:

(a) Core level

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

(b) Professional level

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

4.2 The competency framework for the ECF-ORM with details on the qualifications required and CPD requirement for each job role of a RP is included in Annex 2.

5. Qualification standards and certification

5.1 Qualifications are set in accordance with the following two competency standards:

(a) Core Level
This level of qualification can be met by completing Module 1 to Module 3 of the ECF-ORM Core Level training programme. RPs who have passed the training programmes as specified in Annex 2 are eligible to apply for exemption on Module 1 and/or Module 3.

(b) Professional Level
This level of qualification can be met by completing Module 4 of the ECF-ORM Professional Level training programme on top of the Core Level qualification and having at least 5 years of relevant work experience[2] in operational risk management, business function risk and control gained from AIs and/or non-bank financial institutions as specified in Annex 1, and/or internal audit (related to operational risk management and controls within an AI).

Details of the learning outcomes and syllabus are set out in Annex 3.

5.2 Upon attaining the above qualifications and fulfilling the minimum relevant work experience requirement, RPs may apply to the administrator of the ECF-ORM, the Hong Kong Institute of Bankers (HKIB), for certification as an Associate Operational Risk Management Professional (AORP) or a Certified Operational Risk Management Professional (CORP).

(a) AORP
Successful completion of Module 1 to Module 3 of the Core Level certification; or grandfathered pursuant to paragraph 7.1(a).

(b) CORP
On top of the Core Level certification, successful completion of Module 4 of the

[2] In general, the administrator of the ECF-ORM will consider whether the nature of work experience is substantially the same as that described in the operational risk management roles 1 and 2 in Annex 1. Relevant work experience may be obtained from AIs and/or non-bank financial institutions. As for work experiences related to operational risk management gained from other non-banking industries, they will be considered on a case-by-case basis.

Professional Level certification plus 5 years of relevant experience[3] in operational risk management, business function risk and control gained from AIs and/or non-bank financial institutions as specified in Annex 1, and/or internal audit (related to operational risk management and controls within an AI); or grandfathered pursuant to paragraph 7.1(b). The 5 years of relevant work experience[4] required for CORP certification should be accumulated within the 10 years immediately prior to the date of application for certification, but it does not need to be continuous.

5.3 The ECF-ORM certification is subject to annual renewal by the HKIB together with the renewal of the certificate holder's membership of the HKIB. A RP is required to:

(a) Complete the annual CPD requirement; and

(b) Pay an annual certification fee to renew his/her ECF-ORM certificate.

5.4 The ECF-ORM is referenced to the Hong Kong Qualifications Framework (QF), with the Core Level and the Professional level training programmes mapped at QF Level 4 (i.e. equivalent to associate degree or higher diploma) and QF Level 5 (i.e. equivalent to bachelor's degree) respectively.

6. Training programmes and examinations

6.1 RPs can meet the ECF-ORM benchmark by:

(a) undertaking training programmes offered by the HKIB or other accredited training programmes; and

(b) passing certification examinations hosted by the HKIB.

7. Grandfathering

7.1 A RP may be grandfathered on a one-off basis based on his or her years of qualifying work experience and/or professional qualification. Such work experience need not be continuous. The detailed grandfathering requirements are as follows:

a) Core Level via Path (i) or Path (ii):

[3] Please see footnote 2.

[4] Please see footnote 2.

Path (i):

- Possessing at least 3 years of relevant work experience[5] in operational risk management, business function risk and control gained from AIs and/or non-bank financial institutions, and/or internal audit (related to operational risk management and controls within an AI); and

- Employed by an AI at the time of application.

OR

Path (ii):

- Completion of one of the following training programmes:
  - 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;

- Possessing at least 2 years of relevant work experience[6] in operational risk management, business function risk and control gained from AIs and/or non-bank financial institutions, and/or internal audit (related to operational risk management and controls within an AI); and

- Employed by an AI at the time of application.

b) Professional Level via Path (i) or Path (ii):

Path (i):

- Possessing at least 8 years of relevant work experience[7] in operational risk management, business function risk and control gained from AIs and/or non-bank financial institutions, and/or internal audit (related to operational risk management and controls within an AI), of which at least 3 years must be gained from Professional Level job roles within an AI; and

- Employed by an AI at the time of application.

OR

[5] Please see footnote 2.

[6] Please see footnote 2.

[7] Please see footnote 2.

Path (ii):

- Completion of HKIB's Postgraduate Diploma for Certified Banker (Operations Management Stream); and

- Possessing at least 5 years of relevant work experience[8] in operational risk management, business function risk and control gained from AIs and/or non-bank financial institutions, and/or internal audit (related to operational risk management and controls within an AI); and

- Employed by an AI at the time of application.

7.2 Existing RPs who meet the above criteria can submit their grandfathering applications to the HKIB, the administrator of the ECF-ORM, from 1 July 2021 to 30 June 2022. A one-off grandfathering fee will apply.

7.3 For other individuals who have the relevant work experience but are not working in an AI during the grandfathering period, they may submit their applications to the HKIB for grandfathering within three months from the date of joining the operational risk management function of an AI and becoming a RP. However, they should have met all the applicable grandfathering criteria on or before 30 June 2022 as prescribed above.

7.4 Applications for grandfathering are handled and assessed by the HKIB. The HKIB may request for the applicant to provide employment records or additional information to substantiate the application for grandfathering. Late application will not be accepted.

8. Continuing professional development (CPD)

8.1 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 hours should be on topics related to compliance, legal and regulatory requirements, risk management and ethics.

8.2 Any excess CPD hours accumulated within a particular year cannot be carried forward to the following year.

8.3 Activities that qualify for CPD include:

(a) Attending seminars or courses provided by AIs, financial services regulators,

[8] Please see footnote 2.

professional bodies, academic and training institutions, and the HKIB;

(b) Taking professional examinations;

(c) Attending e-learning (with assessment); and

(d) Delivering training and speeches.

8.4 CPD training topics should be 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

(h) subject areas covered in the HKIB's professional examinations

8.5 The annual CPD requirements are also applicable to RPs meeting the ECF-ORM benchmark through the grandfathering route.

8.6 The CPD requirements will be waived for the first calendar year (ending 31 December) of certification and grandfathering.

8.7 The list of CPD activities and training topics are subject to the HKIB's review from time to time. For details, please refer to the HKIB's website (https://www.hkib.org/).

9. Maintenance of relevant records

9.1 AIs should keep proper records of training, examination, certification and CPD of RPs for monitoring implementation of plan to develop staff competencies or other talent management purposes. AIs are expected to support their staff in their applications for grandfathering and certification. Regarding information related to a RP's previous employment(s), the current employer is encouraged to provide the necessary assistance to the RP in the latter's application for grandfathering or ECF certification (e.g. confirming whether such information is consistent with the curriculum vitae provided by the RP at the time of job application).

9.2 The grandfathering and certification applications would require the Human Resources department of the concerned AI(s) to verify and endorse the relevant work experience reported by an applicant (e.g. name of employer, job position, employment period, total number of years of experience in the relevant functions). An endorsement by the applicant's current employer would indicate that the RP has met the eligibility criteria on relevant work experience before it is passed to the HKIB for processing.

10. Administration of the ECF-ORM

10.1 The HKIB is the administrator of the ECF-ORM. It will be tasked with certifying the qualification required under the ECF-ORM and ensuring that applicants are satisfactorily certified under the specified qualification requirements. The HKIB will also be administering the CPD requirements for ECF-ORM certification holders as set out under the ECF-ORM. For details, please refer to the HKIB's website (https://www.hkib.org/).

11. Accreditation

11.1 The ECF accreditation mechanism is established for interested AIs or education and training operators to have their learning programmes accredited as meeting the ECF standards (including but not limited to the QF Standards) of this ECF module.

11.2 The general criteria for ECF accreditation are as follows:

(a) The learning programme meeting the required standards of individual ECF modules including programme objectives and learning outcomes, programme content and structure, and trainer qualifications and learning mode;

(b) Accreditation of the learning programme at corresponding QF Levels; and

(c) Endorsement by the ECF Steering Committee.

11.3 In order to satisfy criteria 11.2 (a) and (b) outlined above,

(a) For self-accrediting institutions (e.g. institutions funded by the University Grants Committee, including their continuing education arms) / institutions with Hong Kong Council for Accreditation of Academic and Vocational Qualifications (HKCAAVQ) Programme Area Accreditation (PAA) status in related programme areas, they are required to: (i) complete internal quality assurance processes for meeting the relevant ECF standards and the corresponding QF Level and (ii) be assessed by HKCAAVQ as fulfilling the ECF training objectives; and

(b) For other institutions, they are required to complete the accreditation by HKCAAVQ to confirm that their learning programmes can meet the ECF training objectives and the corresponding QF Level.

11.4 HKCAAVQ will accept applications for ECF accreditation starting 2 January 2021.

11.5 Based on the relevant accreditation or assessment report submitted by the applicant, the ECF Steering Committee will confirm whether the training programme is or is not successful in qualifying as an ECF accredited programme. The route for ECF accreditation mechanism is illustrated at Annex 4.

Annex 1 - ECF-ORM: Key roles and tasks for Relevant Practitioners

	Role 1 – Operational Risk Management	**Role 2 – Business Function Risk and Control**
	Core Level *(For entry-level and junior-level staff with 0-5 years of experience)*	
Examples of functional title (for reference only)	Operational risk analyst, assistant operational risk manager	
Key Tasks	• Assist in conducting operational risk monitoring duties (e.g. monitoring operational risk indicators), reviewing and updating operational risk policies, guidelines and procedures, and handling of operational risk events • Assist in conducting operational risk control self-assessments (i.e. bottom up process to identify and evaluate risks and associated controls) • Design and test controls on operational risks, with oversight and input from line managers • Assist in performing operational risk assessments (i.e. top down assessment of the inherent risk and any controls that may exist) • Assist in developing and implementing operational risk mitigation plans and in the roll-out of strategic level governance • Assist in identifying compliance and internal control issues, and monitor the ongoing progress of remedial actions • Assist in preparing operational risk reports, dashboards and metrics • Assist in promoting positive risk culture and risk awareness across the AI /within business units • Assist in preparing training materials and organising training on operational risk for staff	

	Role 1 – Operational Risk Management	**Role 2 – Business Function Risk and Control**
	Professional Level *(For staff taking up middle-level or senior positions in the risk management function with 5+ years of experience)*	
Examples of functional title *(for reference only)*	Operational risk manager	Business risk control manager, in-business control manager, branch operation manager
Key Tasks	• Manage operational risks and formulate, review and update operational risk policies, guidelines, processes and procedures throughout the AI • Develop and review comprehensive policies and procedures for crisis management, including but not limited to factors triggering a crisis, escalation mechanisms, involvement of relevant functions, and external and internal approaches to handling the crisis • Initiate, manage and execute risk governance, internal controls and processes with the overall objective of operational risk management, control awareness and enhancement to operational efficiency. Ensure full compliance with policies and	• Conduct operational risk control self-assessments within business functions (i.e. bottom up process to identify and evaluate risks and associated controls), where applicable • Conduct operational risk assessments to identify, assess, review, monitor and mitigate operational risks within the business function (i.e. top down assessment of the inherent risk and any controls that may exist) • Implement operational risk management and control strategies within the business function as set out by the AI's global risk and compliance functions. Ensure full compliance with policies and regulatory requirements • Analyse business impact of different kinds of

	Role 1 – Operational Risk Management	**Role 2 – Business Function Risk and Control**
	Professional Level *(For staff taking up middle-level or senior positions in the risk management function with 5+ years of experience)*	
	regulatory requirements • Maintain oversight and monitoring of the operational risk management system and the quality of the generated operational loss data • Conduct operational risk control self-assessments (i.e. bottom up process to identify and evaluate risks and associated controls), or analyse and challenge the self-assessment results if the self-assessments are conducted by Role 2 (whichever is applicable) • Conduct operational risk assessments to identify, assess, review, monitor and mitigate operational risks (i.e. top down assessment of the inherent risk and any controls that may exist in all existing or new material products, processes and systems) based on the AI's own defined operational risk strategy and risk appetite • Perform both qualitative and quantitative monitoring and reporting of the AI's exposure to all types of operational risk, including trend analysis of risk profiles and review of the limits of operational risk regulatory and economic capital • Identify compliance and internal control issues • Execute operational risk monitoring duties and escalate incidents and operational risk events to senior management • Report to senior management the proposed remedial actions of operational risk assessments and monitor the ongoing progress of remedial actions • Report and escalate operational risk events/incidents in a timely manner and monitor issue resolution to ensure timely responses are provided • Compile operational risk reports, dashboards and metrics for management reporting • Undertake scenario analysis/assessment to identify potential operational losses and monitor operational risk profiles and material exposures to losses on an on-going basis • Develop and evaluate effectiveness of business continuity and disaster recovery strategy • Provide practical recommendations on the remedial actions to be taken to address	disasters or crisis • Implement and maintain operational risk tools, dashboards and metrics to identify, analyse and mitigate operational risk within the business function • Develop operational risk control measures • Assist management in maintaining oversight on key operational risks, controls and enhancement initiatives and ensure effective and efficient internal controls and practices are in place • Facilitate the testing of relevant controls as a part of the annual test plan and business continuity plan when required • Identify compliance and internal control issues within business functions • Conduct operational risk monitoring duties and escalate incidents and risk events to operational risk management unit and senior management • Report to senior management and operational risk management unit the progress of remedial actions of operational risk assessments • Report and escalate operational risk events/incidents within business functions in a timely manner and monitor issue resolution to ensure timely responses are provided • Manage and provide oversight of completion of follow-up and remedial actions (e.g. further investigation) relating to operational risk events identified during the operational risk assessment process • Assist management in maintaining oversight on key operational risks, controls and enhancement initiatives and ensure effective and efficient internal controls and practices are in place • Liaise and coordinate with other control functions on standards and regulatory interpretation, and operational risk and control activities • Monitor completion of follow-up and remedial actions relating to operational risk incidents and events • Monitor and review the limits of operational risk regulatory and economic capital • Promote positive risk culture and risk awareness in different business units

	Role 1 – Operational Risk Management	**Role 2 – Business Function Risk and Control**
	Professional Level *(For staff taking up middle-level or senior positions in the risk management function with 5+ years of experience)*	
	operational risk events, assess the quality and appropriateness of remedial actions identified and seek to improve the overall operational risk management process for the AI • Manage completion of follow-up actions (e.g. further investigation) relating to operational risk events identified during the operational risk assessment process • Conduct operational due diligence to ensure that operational risk management has been appropriately considered and implemented for new products and services, including thematic reviews of operational risk management • Advise business units on operational risk management issues • Undertake consistent liaison and collaboration with: - Internal departments such as legal, human resources, information technology and finance on operational risk related topics - Operational risk management subject matter experts (e.g. IT, Conduct, Fraud, Outsourcing, Data Privacy) - Internal audit and external audit • Promote positive risk culture and risk awareness across the AI • Conduct training sessions on operational risk for staff, including content review and training delivery	• Play an active role in training sessions on operational risk for staff, including content review and training delivery

Annex 2 - ECF-ORM: Competency framework

	Role 1 – **Operational Risk Management**	**Role 2 –** **Business Function Risk and Control**
	Core Level	
Qualification and experience	• Completion of Module 1 to Module 3 of the ECF-ORM Core Level training programme (benchmarked at the QF Level 4)	
Certification title	• Associate Operational Risk Management Professional (AORP)	
Exemption	RP who has passed the following related training programme(s) is eligible to apply for exemption on **Module 1** of the ECF-Operational Risk Management Core Level training programme: • 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 Diploma for Certified Banker (Stage I) of the 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) RP who has passed the following related training programme(s) is eligible to apply for exemption on **Module 3** of the ECF-Operational Risk Management Core Level training programme: • 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 (Remarks: Other equivalent academic/professional qualifications in operational risk management may be considered for exemption on Module 1 and/or Module 3 on a case-by-case basis. RPs will need to provide detailed information on such qualifications (e.g. training course syllabus, examination syllabus) to the HKIB to facilitate their assessment.)	
Grandfathering (on a one-off basis)	Path (i) • Possessing at least 3 years of relevant work experience in operational risk management, business function risk and control gained from AIs and/or non-bank financial institutions, and/or internal audit (related to operational risk management and controls within an AI); and • Employed by an AI at the time of application. **OR** Path (ii) • Completion of one of the following training programmes: - Operational Risk Manager Certificate of the PRMIA; or - Professional Risk Manager of the PRMIA; or - Certificate in Operational Risk Management of the IOR, which is now a part of the IRM Group; • Possessing at least 2 years of relevant work experience in operational risk management, business function risk and control gained from AIs and/or non-bank financial institutions, and/or internal audit (related to operational risk management and controls within an AI); and	

	• Employed by an AI at the time of application.
CPD requirements	• A minimum of 12 CPD hours is required for each calendar year, of which at least 6 hours should be on topics related to compliance, legal and regulatory requirements, risk management and ethics • Qualified CPD activities include attending seminars or courses provided by AIs, financial services regulators, professional bodies and academic and training institutions and the HKIB; attending e-learning; and delivering training and speeches

	Role 1 – Operational Risk Management	Role 2 – Business Function Risk and Control
	Professional Level	
Qualification and experience	• Completion of Module 4 of the ECF-ORM Professional Level training programme (benchmarked at QF Level 5) on top of the Core Level qualification; and • Having at least 5 years of relevant work experience in operational risk management, business function risk and control, and/or internal audit (related to operational risk management and controls within an AI)	
Certification title	• Certified Operational Risk Management Professional (CORP)	
Grandfathering (on a one-off basis)	Path (i) • Possessing at least 8 years of relevant work experience in operational risk management, business function risk and control gained from AIs and/or non-bank financial institutions, and/or internal audit (related to operational risk management and controls within an AI), of which at least 3 years must be gained from Professional Level job roles within an AI; and • Employed by an AI at the time of application **OR** Path (ii) • Completion of HKIB's Postgraduate Diploma for Certified Banker (Operations Management Stream); and • Possessing at least 5 years of relevant work experience in operational risk management, business function risk and control gained from AIs and/or non-bank financial institutions, and/or internal audit (related to operational risk management and controls within an AI); and • Employed by an AI at the time of application.	
CPD requirements	• A minimum of 12 CPD hours is required for each calendar year, of which at least 6 hours should be on topics related to compliance, legal and regulatory requirements, risk management and ethics • Qualified CPD activities include attending seminars or courses provided by AIs, financial services regulators, professional bodies and academic and training institutions and the HKIB; attending e-learning; and delivering training and speeches	

Annex 3 - ECF-ORM: Learning outcomes and syllabus

Learning outcomes

Core Level (Benchmarked at QF Level 4)

Module 1 – Ethics and Corporate Governance in Banking Industry
Module 2 – Regulatory Framework and Compliance in Banking Industry
Module 3 – Fundamentals of Operational Risk Management and Risk Governance

Learning outcomes - after completing Modules 1 to 3, participants will be able to:

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

Professional Level (Benchmarked at QF Level 5)

Module 4 –Advanced Operational Risk Management

Learning outcomes - after completing Module 4, participants will be able to:

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

Syllabus

Core Level (Benchmarked at QF Level 4)

Module 1 – Ethics and Corporate Governance in Banking Industry

- Business ethics
  - Understand business ethics, their place within modern financial institutions, ethical questions encountered in the second line of defence in the context of the broader risk environment
  - Provide understanding of identification and analysis of ethical situations in financial institutions and the management of ethics
  - Overview of ethical behaviour application and ethical decision making in the second line of defence in the context of the broader risk environment
- Understanding governance, risk and compliance
  - Fundamentals of governance, risk and regulatory compliance and why there is a need to understand the regulatory landscape for financial institutions
  - Key tenets of governance and culture for effective management of regulatory compliance e.g. why risk management is the key to effective compliance
  - The role of the compliance department and compliance professionals in Governance, Risk and Compliance
- Corporate governance in banking industry and requirements mandated upon AIs
  - Corporate Governance Code (for listed AIs)
  - Code of conduct, common policies and procedures
  - Corporate social responsibility
- Case studies, best practices and challenges associated with ethics and corporate governance in the banking industry

Module 2 – Regulatory Framework and Compliance in Banking Industry

- Overview of the regulatory framework under the Hong Kong Monetary Authority, the Securities and Futures Commission and the Insurance Authority
  - Overview of the regulatory regimes in Hong Kong, providing an understanding of how regulations and applicable laws impact the operations of financial institutions
- HKMA Bank culture reform (Governance, Incentive systems, Assessment and Feedback mechanisms)
- Introduction to international regulation (roles of regulator, regulatory powers, different international regulatory models, latest market trends)
- Regulatory objectives and relevant mandates
  - Personal Data (Privacy) Ordinance
  - EU General Data Protection Regulation (GDPR)
  - Code of Banking Practice
  - Code of Conduct for Persons Licensed by or Registered with the Securities and Futures Commission
  - Common Reporting Standards (CRS)
- Supervisory approach and Manager-In-Charge (MIC) Regime
  - Specific overview of the MIC regime and the compliance implications upon AIs in Hong Kong
- Formulation of internal policies, standards and guidelines
  - An overview of best practices in the implementation of internal governance documents (including internal policies, standards and guidelines) to ensure compliance with regulatory frameworks
- Registration and licensing requirements, including listing rules (for listed AIs)
  - The process that needs to be undertaken to ensure compliance with registration and licensing regulations
- Examples of regulatory breaches associated with operational risk incidents
- Case studies, best practices and challenges associated with adapting to regulatory changes in the banking industry

Module 3 – Fundamentals of Operational Risk Management and Risk Governance

- Overview and definition of operational risk
- Drivers of operational risk (e.g. processes, people, systems and external events)
- Different types of operational risks
  - Conduct, External events, Financial Crime, Fraud, Legal and Compliance, Information Technology
- Operational risk events and their consequences
- Relationship between operational risk and other types of risks
- Components of the risk framework and governance structure
- Overview of three lines of defence model - Roles and responsibilities of risk management and control functions

and their interdependence

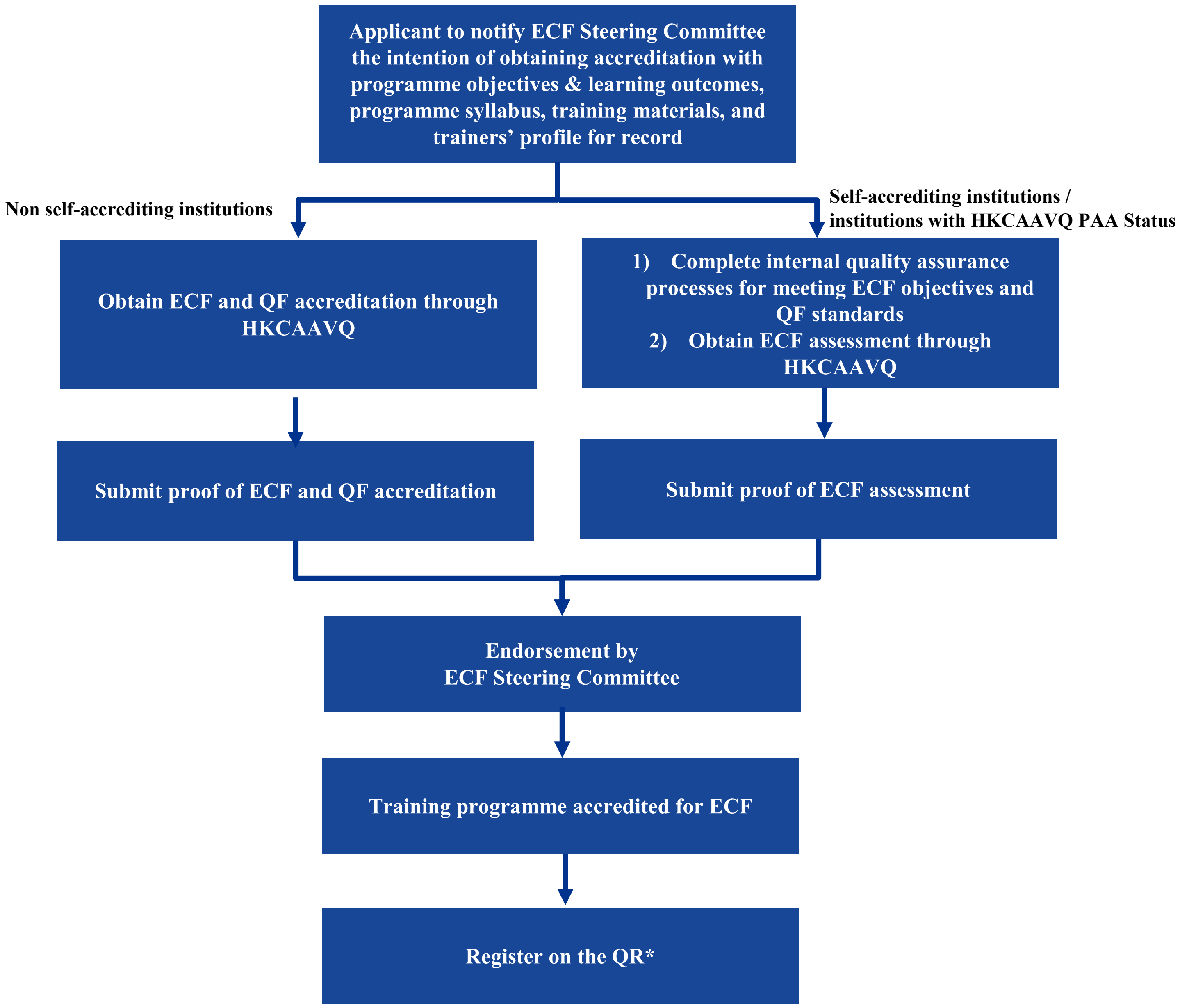
- Roles and responsibilities of the Board and senior management
- Effective risk culture and indicators
- Development of risk governance in the market and emerging operational risks
- Principles of operational risk management framework and implementation (including risk governance frameworks, risk identification and assessment, risk control and mitigation, risk monitoring and reporting, and business resiliency and continuity planning)
- Operational risk management policy and procedures (including principles, application and scope)
  - Operational risk planning and processes
  - Operational risk appetite framework
  - Operational risk impact
- Overview of operational risk measurement – frequency and severity
  - Overview of operational risk assessment
  - Overview of operational risk reporting and dashboards
- Understanding financial products offered in the banking industry and their operational risk implications
- Technology risk management, such as cybersecurity, data privacy and protection, IT change and system disruption, including examples of control activities
- Overview of disaster recovery and business continuity plans
- Enterprise risk management framework
- Case studies, best practices and challenges associated with operational risk management and risk governance

Professional Level (Benchmarked at QF Level 5)

Module 4 – Advanced Operational Risk Management

- Operational risk assessment
- Scenario modelling and analysis, sensitivity testing
  - Stress testing (Value at Risk, Extreme Market Conditions)
- Key risk indicators (KRIs), Key performance indicators (KPIs), Key control indicators (KCI) and respective metrics
- Capital requirements for operational risk – approaches under the Basel framework (including the existing approaches - Basic Indicator Approach (BIA), Standardised Approach (SA), Alternative Standardised Approach (ASA) and Advanced Measurement Approach (AMA), and the Revised Standardised Approach that is scheduled to come into effect from 2022 based on the implementation timetable of the Basel Committee on Banking Supervision (BCBS))
- Risk control self-assessment (RCSA) (e.g. workflow, methodology, toolkits)
  - Operational risk process and control analysis
  - Process risk mapping and control, business process management tools
  - Operational risk reporting and dashboards
- Operational due diligence of new products and services
- Incident and loss reporting, loss (internal and external) data collection, distribution and analysis
- Requirements to ensure adherence to regulatory and supervisory frameworks for Authorised Institutions
  - Compliance with regulatory standards
  - Supervisory approach of regulators
  - On-site examination and prudential meetings
- Building contingency, business continuity and recovery planning
- Guidelines from the BCBS
  - Principles for the Sound Management of Operational Risk
- Associated operational risks related to the key areas for future banking including green and sustainable banking, and digital banking services
- Key components of successful operational risk management implementation
  - Importance and application of trainings in operational risk management
  - Communication and engagement plan of operational risk management in the workplace
  - Communication with senior management on operational risk topics
- Oversight, monitoring and understanding of relevant Operational Risk Management processes taken up by subject matter experts (e.g. IT, Conduct, Fraud, Outsourcing, Data Privacy)
- Key challenges and the future of operational risk management
- Creating a strong risk culture and awareness
- Case studies, best practices and challenges associated with operational risk assessment

Annex 4 – Accreditation mechanism for the ECF-ORM



Applicant to notify ECF Steering Committee the intention of obtaining accreditation with programme objectives & learning outcomes, programme syllabus, training materials, and trainers' profile for record

Non self-accrediting institutions

Obtain ECF and QF accreditation through HKCAAVQ

Submit proof of ECF and QF accreditation

Self-accrediting institutions / institutions with HKCAAVQ PAA Status

1) Complete internal quality assurance processes for meeting ECF objectives and QF standards
2) Obtain ECF assessment through HKCAAVQ

Submit proof of ECF assessment

Endorsement by ECF Steering Committee

Training programme accredited for ECF

Register on the QR*

*Subject to re-accreditation/re-assessment by HKCAAVQ