



Guideline for ECF on Operational Risk Management (ORM) Certification

Introduction

This document is developed to provide more specific guidelines for the application of the ECF on ORM Certification. It includes information related to (A) Eligibility Criteria, (B) Application Procedure and (C) Recertification Arrangement for the application(s) of the following professional qualifications:

- Associate Operational Risk Management Professional (AORP);
- Certified Operational Risk Management Professional (CORP).

A. Eligibility Criteria

1. Relevant Practitioner

The Enhanced Competency Framework (ECF) on Operational Risk Management (ORM) is targeted at “Relevant Practitioners (RPs)”, engaged by an **Authorized Institution (AI)**¹. The ECF-ORM is intended to apply to staff whose primary responsibilities are performing operational risk governance, operational risk identification and assessment, operation risk monitoring and reporting, operational risk control and mitigation, and business resiliency and continuity planning with an AI.

Specifically, it is aimed at RPs located in the Hong Kong office of an AI who perform the operational risk management job roles. The definition of RPs has taken into account differences among AIs in how operational risk management practitioners are assigned within different organizational 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 roles/ tasks outlined in Annex 1 which is quoted from the HKMA circular on [“Guide to Enhanced Competency Framework on Operational Risk Management”](#).

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 circular on [“Guide to ECF on Cybersecurity”](#) for details of these roles.

¹ An institution authorized under the Banking Ordinance to carry on the business of taking deposits. Hong Kong maintains a Three-tier Banking System, which comprises banks, restricted license banks and deposit-taking companies. Authorized institutions are supervised by the HKMA.



Guideline for ECF on Operational Risk Management (ORM) Certification

- (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).
- (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.

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.

Please refer to HKMA circular on [“Guide to Enhanced Competency Framework on Operational Risk Management”](#) dated 18 December 2020 for more details.

2. Other Certification Requirements

- (a) AORP:
 - Completed 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 of the [“Guide to Enhanced Competency Framework on Operational Risk Management”](#) are eligible to apply for exemption on Module 1 and/or Module 3; or
 - Grandfathered for ECF on ORM (Core Level)
- (b) CORP:
 - On top of the attainment in ECF on ORM (Core Level), successful completion of Module 4 of the ECF-ORM Professional Level training programme plus 5 years of relevant experience* in operational risk management, business function risk and control gained from AIs and/or non-bank financial institutions as specified in Annex 1 of the [“Guide to](#)



Guideline for ECF on Operational Risk Management (ORM) Certification

[Enhanced Competency Framework on Operational Risk Management](#)”, and/or internal audit (related to operational risk management and controls within an AI). The 5 years of relevant work experience* 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; or

- Grandfathered for ECF-ORM (Professional Level)

**In general, HKIB 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 of the [“Guide to Enhanced Competency Framework on Operational Risk Management”](#). Relevant work experience may be obtained from the 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.*

B. Application Procedure

Please follow the application procedure below:

(a) Complete all the necessary fields in the relevant Grandfathering and/or Certification Application Form for ECF on ORM, including applicant’s signature and HR endorsement in relevant sections.

- For Core Level: ORM-G-009
- For Professional Level: ORM-G-010

Note: Applicant is encouraged to apply for both Grandfathering and Certification at one time by using the above application form. Please also read the Guidelines for ECF on ORM Grandfathering (ORM-G-007) if Grandfathering and Certification are applied at same time.

(b) Obtain the endorsement from Human Resources Department (HR) of the concerned Authorized Institution(s) by obtaining his/her signature and company chop on the Annex of the Grandfathering and/or Certification Application Form – HR Department Verification Form on Key Roles/ Responsibilities for ORM Practitioners. Application is only accepted with HR verification.



Guideline for ECF on Operational Risk Management (ORM) Certification

(c) Applicant is required to fill in **ONE** completed HR Verification Form for **EACH** relevant position/ functional title in the application.

Als are expected to support their staff to apply for grandfathering and certification. Regarding information related to a Relevant Practitioner’s previous employment(s), the current employer is encouraged to provide necessary assistance to Relevant Practitioners in the latter’s applications for grandfathering or ECF certification (e.g. confirming whether such information is consistent with the curriculum vitae provided by the Relevant Practitioner at the time of job application).

If required, the HKIB may request the applicant to provide employment records or additional information to substantiate the application for grandfathering.

(d) Read Policy of Personal Data Protection set out on HKIB website before submitting application.

(e) Send the completed Application Form with HR department’s endorsement, relevant supporting documents (e.g. certified true copies of your HKID / Passport, copies of your examination result or grandfathered approval letter for relevant Certificate for ECF on ORM), cheque/ payment evidence to HKIB within the required time frame.

- Time frame for submitting AORP/CORP Certification application

Pathway	Application Deadline
Completed the Core/ Professional Level of the ECF on ORM training modules; passed the examinations and fulfilled the required work experience	8 years of completion period to attend the training, pass the examination and fulfill the required work experience from the year in which the first module was completed for each level. <i>After the application deadline, individuals who do not submit their AORP/ CORP application must retake and pass the corresponding level examinations to recommence the eligibility to apply for AORP/CORP certification.</i>



Guideline for ECF on Operational Risk Management (ORM) Certification

Pathway	Application Deadline
Grandfathered based on the required work experience and qualification	3 months after issuance of the Grandfathering Approval Letter if both grandfathering and respective certification are not applying at the same time. <i>After the application deadline, the grandfathered status is invalid for applying the AORP/CORP certification.</i>

- Fee Payable

For each of the AORP/CORP certification application (**valid until 31 December 2021**):

1st year certification:

- Not currently a HKIB member: HKD1,650
- Current HKIB Student member: HKD1,650
- Current HKIB Ordinary member: HKD570
- Current HKIB Professional member: Waived
- Current HKIB Senior member: HKD1,450

Annual Renewal:

- Certification: HKD1,650
- Reinstatement fee of default member: HKD2,000

Note: Please note that the certification fee is non-refundable.

- Payment Method

- Paid by Employer
- A crossed cheque or e-cheque made payable to "The Hong Kong Institute of Bankers". Postdated cheques will not be accepted.
- Credit card (Visa or Mastercard)



Guideline for ECF on Operational Risk Management (ORM) Certification

- Submission of Application

Please complete and submit the **SIGNED** application form together with the required documents by post/ in person to The Hong Kong Institute of Bankers (HKIB) at the following address:

“Application for ECF on ORM Grandfathering/ Certification”

Department of Professional Assessment and Certification

The Hong Kong Institute of Bankers

3/F Guangdong Investment Tower,

148 Connaught Road, Central, Hong Kong

Note: Please ensure sufficient postage is provided when sending out the required documents.

- Approval and Election

The certification processing time, including the election process done by HKIB committee members, will require around **60 days**. If grandfathering is also applied together with certification by using the combined application form, the processing time will be around **120 days**.

Upon the successful completion of the certification process, AORP/CORP holders will be registered as Certified Individuals (CI) and included in a public register on HKIB website. HKIB will also grant the holder a professional membership. AORP/CORP professional qualification holders are then entitled to print the professional qualification on their business card and curriculum vitae which signifies their professional excellence.

Besides, the professional qualification holders' names will also be presented on HKIB website and published on the Institute's journal “Banking Today” and Annual Report.



Guideline for ECF on Operational Risk Management (ORM) Certification

C. Recertification Arrangement

- (a) Subject to HKIB membership governance, if the applicant wants to apply for and maintain his/her AORP/CORP professional qualification, he/she is required to maintain a valid membership status with HKIB. The applicant must also be a Relevant Practitioner who has met the annual continuing professional development (CPD) requirement and pay the annual renewal of certificate fee.
- (b) AORP/CORP holders would be bound by the prevailing rules and regulations of HKIB. They are abided by HKIB's rules and regulations in HKIB Members' Handbook. AORP/CORP holders are required to notify HKIB of any material changes to responses to any of the questions in application of the certification, including their contact details. HKIB may investigate the statements AORP/CORP holders have made with respect to their applications, and that they may be subject to disciplinary actions for any misrepresentation (whether fraudulent and otherwise) in their applications.
- (c) To maintain ongoing professionalism and standards, both AORP/CORP holders are required to undertake a minimum of **12 CPD hours** each calendar year (ending 31 December) for the highest professional qualification only. At least **6 CPD hours** must be earned from activities related to topics of compliance, legal and regulatory requirements, risk management and ethics. Any excess CPD hours accumulated within a particular year cannot be carried forward to the following year.
- (d) The renewal of AORP/CORP certification is subject to fulfilment of the annual CPD requirements starting from the calendar year (**from 1 January to 31 December**) following the year of certification.
- (e) The annual CPD requirements are also applicable to Relevant Practitioners meeting the ECF on ORM benchmark through the grandfathering route.
- (f) The CPD requirements will be waived for the first calendar year (**ending 31 December**) of certification and grandfathering.

--END--

Guideline for ECF on Operational Risk Management (ORM) Certification

Annex 1: ECF-ORM: Key Roles and Tasks for Relevant Practitioners

(Quoted from the Annex 1 [“Guide to Enhanced Competency Framework on Operational Risk Management”](#))

	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 <i>(for reference only)</i>	Operational risk analyst, assistant operational risk manager	
Key tasks	<ol style="list-style-type: none"> 1. 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 2. Assist in conducting operational risk control self-assessments (i.e. bottom up process to identify and evaluate risks and associated controls) 3. Design and test controls on operational risks, with oversight and input from line managers 4. Assist in performing operational risk assessments (i.e. top down assessment of the inherent risk and any controls that may exist) 5. Assist in developing and implementing operational risk mitigation plans and in the roll-out of strategic level governance 6. Assist in identifying compliance and internal control issues, and monitor the ongoing progress of remedial actions 7. Assist in preparing operational risk reports, dashboards and metrics 8. Assist in promoting positive risk culture and risk awareness across the AI/ within business units 9. 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 <i>(for reference only)</i>	Operational risk manager	Business risk control manager, in-business control manager, branch operation manager
Key tasks	<ol style="list-style-type: none"> 1. Manage operational risks and formulate, review and update operational risk policies, guidelines, processes and procedures throughout the AI 2. Develop and review comprehensive policies and procedures for crisis management, including but not limited to factors triggering a crisis, escalation 	<ol style="list-style-type: none"> 1. Conduct operational risk control self-assessments within business functions (i.e. bottom up process to identify and evaluate risks and associated controls), where applicable 2. Conduct operational risk assessments to identify, assess, review, monitor and mitigate operational risks within the

Guideline for ECF on Operational Risk Management (ORM) Certification

	<p>mechanisms, involvement of relevant functions, and external and internal approaches to handling the crisis</p> <ol style="list-style-type: none"> 3. 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 regulatory requirements 4. Maintain oversight and monitoring of the operational risk management system and the quality of the generated operational loss data 5. 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) 6. 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 7. 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 8. Identify compliance and internal control issues 9. Execute operational risk monitoring duties and escalate incidents and operational risk events to senior management 10. Report to senior management the proposed remedial actions of operational risk assessments and monitor the ongoing progress of remedial actions 11. Report and escalate operational risk events/incidents in a timely manner and monitor issue resolution to ensure timely responses are provided 12. Compile operational risk reports, dashboards and metrics for management 	<p>business function (i.e. top down assessment of the inherent risk and any controls that may exist)</p> <ol style="list-style-type: none"> 3. 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 4. Analyse business impact of different kinds of disasters or crisis 5. Implement and maintain operational risk tools, dashboards and metrics to identify, analyse and mitigate operational risk within the business function 6. Develop operational risk control measures 7. 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 8. Facilitate the testing of relevant controls as a part of the annual test plan and business continuity plan when required 9. Identify compliance and internal control issues within business functions 10. Conduct operational risk monitoring duties and escalate incidents and risk events to operational risk management unit and senior management 11. Report to senior management and operational risk management unit the progress of remedial actions of operational risk assessments 12. Report and escalate operational risk events/incidents within business functions in a timely manner and monitor issue resolution to ensure timely responses are provided 13. 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 14. 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
--	---	---



Guideline for ECF on Operational Risk Management (ORM) Certification

	<p>reporting</p> <p>13. Undertake scenario analysis/assessment to identify potential operational losses and monitor operational risk profiles and material exposures to losses on an on-going basis</p> <p>14. Develop and evaluate effectiveness of business continuity and disaster recovery strategy</p> <p>15. Provide practical recommendations on the remedial actions to be taken to address 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</p> <p>16. Manage completion of follow-up actions (e.g. further investigation) relating to operational risk events identified during the operational risk assessment process</p> <p>17. 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</p> <p>18. Advise business units on operational risk management issues</p> <p>19. Undertake consistent liaison and collaboration with:</p> <ul style="list-style-type: none"> - 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 <p>20. Promote positive risk culture and risk awareness across the AI</p> <p>21. Conduct training sessions on operational risk for staff, including content review and training delivery</p>	<p>15. Liaise and coordinate with other control functions on standards and regulatory interpretation, and operational risk and control activities</p> <p>16. Monitor completion of follow-up and remedial actions relating to operational risk incidents and events</p> <p>17. Monitor and review the limits of operational risk regulatory and economic capital</p> <p>18. Promote positive risk culture and risk awareness in different business units</p> <p>19. Play an active role in training sessions on operational risk for staff, including content review and training delivery</p>
--	--	--