香 港 銀 行 學 會
The Hong Kong Institute of Bankers

Guideline for ECF on Operational Risk Management (ORM) Grandfathering

Introduction

This document is developed to provide more specific guidelines for the grandfathering application of the ECF on ORM at Core and Professional Level. It includes information related to (A) Eligibility Criteria, (B) Application Procedure for Grandfathering, (C) AORP & CORP Certification Requirement and (D) Appeal Arrangement.

A. Eligibility Criteria

1. Scope of application and 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 listed in the table below.

	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	• 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

[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.

	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.	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.

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.

(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. Grandfathering Requirements

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 follow:

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

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 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* 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* 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 the 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.

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.***

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

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 with 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.

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.

B. Application Procedure for Grandfathering

Please follow the application procedure below:

(a) Complete all 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 Certification (ORM-G-008) 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.

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

AIs 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.

- Grandfathering Application Period
  HKIB will accept application for grandfathering by current Relevant Practitioners of AIs from **1 July 2021**. Completed application with all required supporting documents must be submitted to HKIB office. The deadline for application will be **30 June 2022**. Late submission, application with incomplete information and applications by fax/ email will NOT be accepted.

- Fee Payable
  An application fee of HKD1,050 is required for each grandfathering application for both Core and Professional Level respectively

- 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)

- 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

  It is expected to take **60 days** for HKIB to process grandfathering applications with completed submission of documents and information under normal circumstance. If certification is also applied together with grandfathering by using the combined application form, the processing time will be around **120 days**.

  Once grandfathering and/or certification has been granted, the Relevant Practitioner will be notified via email to the applicant.

  Note: The approval of grandfathering is subject to the final decision of the HKIB.

Please refer to the respective Grandfathering and/or Certification Application Forms for ECF on ORM (ORM-G-009 and ORM-G-010) for details and read the Policy of Personal Data Protection set out on HKIB website before application.

3. AORP/ CORP Certification Requirement

For details, applicants can refer to the Guideline for ECF on ORM Certification (ORM-G-008).

4. Appeal Arrangement

HKIB will appoint a Grandfathering of ECF on ORM Appeal Committee (Appeal Committee) as necessary, to handle the appeal of grandfathering applications. The appeal mechanism applies if a formal written notice of appeal, specifying the ground, is sent to the HKIB by the grandfathering applicant whose application has been declined by the HKIB. There will be an administrative fee for appeal application.

(a) Grandfathering Appeal Procedure

Candidates may request in writing for any appeal against their grandfathering result **within 1 month** after the issuance of grandfathering declination letter. An administrative fee would be applied. Late appeal application will not be accepted.

The appellant may be asked to attend the appeal hearing by the Appeal Committee, or provide extra supporting documents if the Committee has any question they wish to ask the appellant. The Appeal Committee meeting will be conducted as required. The Appeal Committee shall decide to either accept the appeal or decline the appeal.

It is expected to take **90 days** for HKIB to process grandfathering appeal application under normal circumstance. The appellant will be notified of the decision by the Appeal Committee in writing and a document will be signed by General Manager of HKIB as record. Candidates will be informed of their appeal results by post and / or email and with written notice for approved case.

(b) Fee Payable

An administrative fee of HKD1,000 is required for the appeal application.

--END--

Guideline for ECF on Operational Risk Management (ORM) Grandfathering

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 *(for reference only)*	Operational risk analyst, assistant operational risk manager	
Key tasks	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 *(for reference only)*	Operational Risk Manager	Business Risk Control Manager In-Business Control Manager Branch Operation Manager
Key tasks	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 mechanisms, involvement of relevant	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 business function (i.e. top down

	functions, and external and internal approaches to handling the crisis 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 reporting 13. Undertake scenario analysis/assessment	assessment of the inherent risk and any controls that may exist) 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 15. Liaise and coordinate with other control functions on standards and regulatory

Guideline for ECF on Operational Risk Management (ORM) Grandfathering

	to identify potential operational losses and monitor operational risk profiles and material exposures to losses on an on-going basis 14. Develop and evaluate effectiveness of business continuity and disaster recovery strategy 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 16. Manage completion of follow-up actions (e.g. further investigation) relating to operational risk events identified during the operational risk assessment process 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 18. Advise business units on operational risk management issues 19. 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 20. Promote positive risk culture and risk awareness across the AI 21. Conduct training sessions on operational risk for staff, including content review and training delivery	interpretation, and operational risk and control activities 16. Monitor completion of follow-up and remedial actions relating to operational risk incidents and events 17. Monitor and review the limits of operational risk regulatory and economic capital 18. Promote positive risk culture and risk awareness in different business units 19. Play an active role in training sessions on operational risk for staff, including content review and training delivery