

From the Banking Regulation and Supervision Agency:

**COMMUNIQUÉ ON CALCULATION OF THE RISK WEIGHTED
EXPOSURE AMOUNT FOR OPERATIONAL RISK BY ADVANCED
MEASUREMENT APPROACH**

(Published in the Official Gazette dated November 6, 2014, Nr 28812)

SECTION ONE

Purpose and Scope, Legal Basis and Definitions

Purpose and Scope

ARTICLE 1- (1) The purpose of this Communiqué is to set down the procedures and principles regarding the banks' calculation of risk weighted exposure amount for operational risk using advanced measurement approach.

Legal Basis

ARTICLE 2- (1) This communiqué is based on Articles 43, 45 and 93 of Banking Law Nr. 5411 dated October 19, 2005 and Article 23 of Regulation on Measurement and Evaluation of Capital Adequacy of Banks published in the Official Gazette Nr. 28337 dated 28/06/2014.

Definitions and Abbreviations

ARTICLE 3- (1) The following terms and expressions used in this Communiqué must have the meanings expressly designated to them below:

- a) Bank: Banks as defined in Article 3 of the Law,
- b) Law: Banking Law Nr. 5411,
- c) Agency: Banking Regulation and Supervision Agency,
- ç) Credit rating agency (CRA): Credit rating agency as defined in Article 3 of the Regulation,
- d) Operational risk: Operational risk as defined in Article 3 of the Regulation,
- e) Risk profile: Risk profile as defined in Article 3 of the Regulation,
- f) Regulation: Regulation on Measurement and Evaluation of Capital Adequacy of Banks,

SECTION TWO

Provisions Regarding Advanced Measurement Approach

Supervisory permission period regarding Advanced Measurement Approach

ARTICLE 4- (1) Prior permission from Agency is required in order to use the Advanced Measurement Approach provided that all the qualitative and quantitative standards set out in Articles 5 and 6 respectively are met, contingency and business continuity plans sufficiently in place as set out in Regulation on Internal Systems as well as Internal Capital Adequacy Evaluation Process of Banks and banks meet general operational risk management standards as set out in article 35 of the same Regulation.

(2) Banks must also apply for permission from Agency where they want to implement material extensions and changes to those Advanced Measurement Approaches. Agency shall grant the permission only where banks would continue to meet the standards specified in the first subparagraph following those material extensions and changes.

(3) Banks must notify the Agency of all changes to their Advanced Measurement Approaches models.

Qualitative standards regarding Advanced Measurement Approach

ARTICLE 5- (1) The following qualitative standards must be satisfied.

a) A bank's internal operational risk measurement system must be closely integrated into its day-to-day risk management processes. This measurement system must also be capable of supporting an allocation of economic capital for operational risk across business lines in a manner that creates incentives to improve business line operational risk management and banks must have techniques for these purposes.

b) A bank must have an independent operational risk management function which is performed by risk management unit or by a unit which is organized under the same internal systems manager that risk management unit is related.

c) There must be regular reporting of operational risk exposures and loss experience to business unit management, senior management, and to the board of directors. The bank must have procedures for taking appropriate action according to the information within the management reports.

ç) A bank's risk management system must be well documented. A bank must have in place routines for ensuring compliance and policies for the treatment of non-compliance.

d) Internal auditors must perform regular reviews of the operational risk management processes and measurement systems. This review must include both the activities of the business units and of the independent operational risk management function.

e) The validation of the operational risk measurement system must include the followings.

(i) Verifying that the internal validation processes are operating in a satisfactory manner.

(ii) Making sure that data flows and processes associated with the risk measurement system are transparent and accessible. It is necessary that Agency is in a position to have easy Access to the system's specifications and parameters.

Quantitative standards regarding Advanced Measurement Approach

ARTICLE 6- (1) The quantitative standards include the standards relating to process, to internal data, to external data, to scenario analysis, to business environment and to internal control factors laid down in paragraphs 2 to 6 respectively.

(2) The standards relating to process are the following:

(a) The operational risk measure must capture potentially severe tail events, achieving a soundness standard comparable to a 99,9 % confidence interval over a one year period.

b) Operational risk measurement system must include the use of internal data, external data, scenario analysis and factors reflecting the business environment and internal control systems as set out in paragraphs 3 to 6. A bank needs to have a credible, transparent, and

verifiable approach for weighting these four fundamental elements in its overall operational risk measurement system and this approach must be well documented. The bank's approach for weighting the four fundamental elements should be internally consistent and avoid the double counting of qualitative assessments or risk mitigants already recognised in other elements of the framework.

c) Operational risk measurement system must capture the major drivers of risk affecting the shape of the tail of the estimated distribution of losses.

ç) Correlations in operational risk losses across individual operational risk estimates can be recognised only where its systems for measuring correlations are sound, implemented with integrity, and take into account the uncertainty surrounding any such correlation estimates, particularly in periods of stress. Correlation assumptions using appropriate quantitative and qualitative techniques must be validated by banks.

(3) The standards relating to internal data are the following.

a) Internally generated operational risk measures used for regulatory capital purposes must be based on a minimum five-year observation period of internal loss data.

b) Historical internal loss data must be mapped into the bank's business lines defined in Article 25 of the Regulation, and into the event types defined in Article 9, and to provide these data to Agency upon request.

c) Banks must have documented, objective criteria for allocating losses to the specified business lines and event types.

ç) Operational risk losses that are related to credit risk and have historically been included in banks' credit risk databases will be also included within a bank's internal operational risk database and viewed separately. If these losses are treated as credit risk for the purposes of calculating minimum regulatory capital then they are not included to calculation of operational risk regulatory capital requirement.

d) Operational risk losses that are related to market risks are included to the scope of the capital requirement for operational risk.

e) A bank's internal loss data must be comprehensive in that it captures all material activities and exposures. Activities or exposures that would not have a material impact on the overall risk can be excluded provided that these are justified by banks. A bank must be able to justify that any excluded activities or exposures, both individually and in combination, would not have a material impact on the overall risk estimates. A bank must define an appropriate *de minimis* gross loss threshold and internal loss data collection must be done according to this threshold.

f) Aside from information on gross loss amounts, a bank should collect information about the date of the event, if this date can not be determined collect information about the transaction's accounting date, any recoveries of gross loss amounts, as well as some descriptive information about the drivers or causes of the loss event. The level of detail of any descriptive information should be commensurate with the size of the gross loss amount.

g) Specific criteria for assigning loss data arising from a loss event in a centralised function or an activity that spans more than one business line, as well as from related loss events over time must be determined.

ğ) A bank must have in place documented procedures for assessing the on-going relevance of historical loss data, including those situations in which judgement overrides,

scaling, or other adjustments may be used, to what extent they may be used and who is authorised to make such decisions.

(4) The qualifying standards relating to external data are the following.

a) A bank's operational risk measurement system must use relevant external data, especially when there is reason to believe that the bank is exposed to infrequent, yet potentially severe, losses. These external data should include data on actual loss amounts, information on the scale of business operations where the event occurred, information on the causes and circumstances of the loss events or other information that would help in assessing the relevance of the loss event for other banks. A bank must have a systematic process for determining the situations for which external data must be used and the methodologies used to incorporate the data.

b) The conditions and practices for external data use must be regularly reviewed, documented, and subject to periodic independent review.

(5) A bank must use scenario analysis of expert opinion in conjunction with external data to evaluate its exposure to high-severity events. In addition, scenario analysis should be used to assess the impact of deviations from the correlation assumptions embedded in the bank's operational risk measurement framework, in particular, to evaluate potential losses arising from multiple simultaneous operational risk loss events. Over time, such assessments need to be validated and re-assessed through comparison to actual loss experience to ensure their reasonableness.

(6) The qualifying standards relating to business environment and internal control factors are the following.

a) A bank's operational risk assessment methodology must capture key business environment and internal control factors that can change the bank's operational risk profile.

b) The choice of each factor needs to be justified as a meaningful driver of risk, based on experience and involving the expert judgment of the affected business areas. Whenever possible, the factors should be translatable into quantitative measures that lend themselves to verification.

c) The sensitivity of a bank's risk estimates to changes in the factors and the relative weighting of the various factors need to be well reasoned. In addition to capturing changes in risk due to improvements in risk controls, the framework must also capture potential increases in risk due to greater complexity of activities or increased business volume.

ç) Risk measurement framework must be documented and subject to independent review by internal audit. Over time, the process and the outcomes need to be validated through comparison to actual internal loss experience, relevant external data, and appropriate adjustments made.

Risk weighted exposure amount for operational risk

ARTICLE 7- (1) Sum as a basis for operational risk is calculated as the sum of both expected loss and unexpected loss multiplied by 12,5. If expected loss is adequately captured with provision, then this amount of expected loss is not included to calculation. The sum as a basis for operational risk calculated according to this Communiqué will not be less than 70% of the sum as a basis for operational risk calculated by according to Basic Indicator Approach.

Risk Mitigation regarding operational risk

ARTICLE 8- (1) Banks must recognise the impact of insurance subject to the conditions set out in paragraphs 2 to 5 where the bank can demonstrate that a noticeable risk mitigating effect is achieved.

(2) The insurance provider must be authorised to provide insurance or re-insurance and have a minimum claims paying ability rating by an CRA to be associated with credit quality step 2 or above under the rules for the risk weighting of exposures to banks and investment firms under Annex-1 of Regulation.

(3) The insurance and the insurance framework must meet all the following conditions.

a) The insurance policy must have an initial term of no less than one year. For policies with a residual term of less than one year, the bank must make appropriate haircuts reflecting the declining residual term of the policy, up to a full 100% haircut for policies with a residual term of 90 days or less.

b) The insurance policy has a minimum notice period for cancellation of 90 days.

c) The insurance policy has no exclusions or limitations triggered by Agency actions or, in the case of a failed bank, that preclude the bank, receiver or liquidator from recovering for damages suffered or expenses incurred by the bank, except in respect of events occurring after the initiation of receivership or liquidation proceedings in respect of the bank provided that the insurance policy may exclude any fine, penalty, or punitive damages resulting from Agency actions.

ç) The risk mitigation calculations must reflect the bank's insurance coverage in a manner that is transparent in its relationship to, and consistent with, the actual likelihood and impact of loss used in the bank's overall determination of its operational risk capital.

d) The insurance is provided by a third-party entity . In the case of insurance through captives and affiliates, the exposure has to be laid off to an independent third-party entity, for example through re-insurance, that meets the eligibility criteria set out in paragraph 2.

e) The framework for recognising insurance is well reasoned and documented.

(4) A bank's methodology for recognising insurance also needs to capture the following elements through appropriate discounts in the amount of insurance recognition.

a) The residual term of a policy, where less than one year.

b) A policy's cancellation terms, where less than one year.

c) The uncertainty of payment as well as mismatches in coverage of insurance policies.

(5) The recognition of insurance mitigation will be limited to 20% of the total risk weighted exposure amount for operational risk.

Loss event type classification

ARTICLE 9- (1) The loss events types referred to in point (b) to (d) of Article 6(3) are the following.

Loss Event	Definition of Losses	Categories	Activity Examples
Internal fraud	Losses due to acts of a type intended to defraud, misappropriate property or circumvent regulations, the law or company policy, excluding diversity or discrimination events, which involves at least one internal party	Unauthorised Activity	Transactions not reported (intentional) Transaction type unauthorised (w/monetary loss) Mismarking of position (intentional)
		Theft and Fraud	Fraud / credit fraud / worthless deposits Theft / extortion / embezzlement / robbery Misappropriation of assets Malicious destruction of assets Forgery Check kiting Smuggling Account take-over / impersonation / etc. Tax non-compliance / evasion Bribes / kickbacks Insider trading (not on firm's account)
External fraud	Losses due to acts of a type intended to defraud, misappropriate property or circumvent the law, by a third party	Theft and Fraud	Theft/Robbery Forgery Check kiting
		Systems Security	Hacking damage Theft of information (w/monetary loss)
Employment Practices and Workplace Safety	Losses arising from acts inconsistent with employment, health or safety laws or agreements, from payment of personal injury claims, or from diversity or discrimination events	Employee Relations	Compensation, benefit, termination issues Organised labour activity
		Safe Environment	General liability Employee health and safety rules events Workers compensation
		Diversity and Discrimination	All discrimination types
Clients, Products and Business Practices	Losses arising from an unintentional or negligent failure to meet a professional obligation to specific clients, or from the nature or design of a product.	Suitability, Disclosure and Fiduciary	Fiduciary breaches / guideline violations Suitability / disclosure issues Retail customer disclosure violations Breach of privacy Aggressive sales Account churning Misuse of confidential information Lender liability
		Improper Business or Market Practices	Antitrust Improper trade / market practices Market manipulation Insider trading (on firm's account) Unlicensed activity Money laundering
		Product Flaws	Product defects Model errors
		Selection, Sponsorship and Exposure	Failure to investigate client per guidelines Exceeding client exposure limits
		Advisory Activities	Disputes over performance of advisory activities
Damage to Physical Assets	Losses arising from loss or damage to physical assets from natural disaster or other	Disasters and other events	Natural disaster losses Human losses from external sources (terrorism, vandalism)

	events		
Business disruption and system failures	Losses arising from disruption of business or system failures	Systems	Hardware Software Telecommunications Utility outage / disruptions
Execution, Delivery and Process Management	Losses from failed transaction processing or process management, from relations with trade counterparties and vendors	Transaction Capture, Execution and Maintenance	Miscommunication Data entry, maintenance or loading error Missed deadline or responsibility Model / system misoperation Accounting error / entity attribution error Other task misperformance Delivery failure Collateral management failure Reference Data Maintenance
		Monitoring and Reporting	Failed mandatory reporting obligation Inaccurate external report (loss incurred)
		Customer Intake and Documentation	Client permissions / disclaimers missing Legal documents missing / incomplete
		Customer / Client Account Management	Unapproved access given to accounts Incorrect client records (loss incurred) Negligent loss or damage of client assets
		Trade Counterparties	Non-client counterparty misperformance Misc. non-client counterparty disputes
		Vendors and Suppliers	Outsourcing Vendor disputes

SECTION THREE

Provisional and Final Provisions

PROVISIONAL ARTICLE 1- (1) In implementation of paragraph 3(a) of Article 6, a three-year historical data window is acceptable starting from the date of the Communiqué entry into force. This window has increased every year until rdata period reaches to 5 years.

Entry into Force

ARTICLE 10- This Communiqué enter into force as of the date 1/1/2015.

Enforcement

ARTICLE 11- (1) The provisions of this Communiqué are enforced by the Chairman of the Banking Regulation and Supervision Agency.