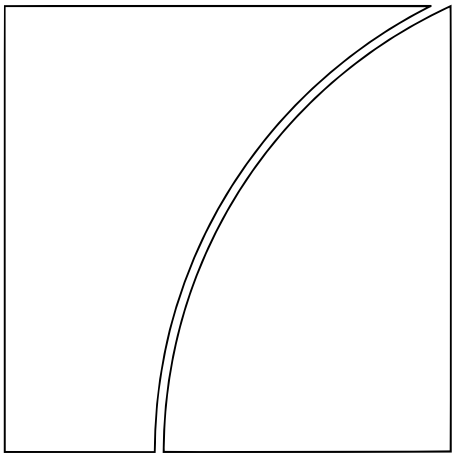
Basel Committee on Banking Supervision

OPE

Calculation of RWA for operational risk

OPE30



Advanced Measurement Approaches

This chapter describes the criteria that banks must meet to be able to calculate operational risk capital requirements based on internal risk measurement systems.

Version effective as of 15 December 2019

First version in the format of the consolidated framework.

BANK FOR INTERNATIONAL SETTLEMENTS

This document has been generated on 23/11/2026 based on the Basel Framework data available on the BIS website (www.bis.org).

© Bank for International Settlements 2026. All rights reserved.

Introduction

30.1

Under the Advanced Measurement Approaches (AMA), the regulatory capital requirement will equal the risk measure generated by the bank's internal operational risk measurement system using the quantitative and qualitative criteria for the AMA discussed below. Use of the AMA is subject to supervisory approval.

30.2

A bank adopting the AMA may, with the approval of its host supervisors and the support of its home supervisor, use an allocation mechanism for the purpose of determining the regulatory capital requirement for internationally active banking subsidiaries that are not deemed to be significant relative to the overall banking group but are themselves subject to this Framework in accordance with SCO10. Supervisory approval would be conditional on the bank demonstrating to the satisfaction of the relevant supervisors that the allocation mechanism for these subsidiaries is appropriate and can be supported empirically. The board of directors and senior management of each subsidiary are responsible for conducting their own assessment of the subsidiary's operational risks and controls and ensuring the subsidiary is adequately capitalised in respect of those risks.

30.3

Subject to supervisory approval as discussed in [[OPE30.11]](4), the incorporation of a well-reasoned estimate of diversification benefits may be factored in at the group-wide level or at the banking subsidiary level. However, any banking subsidiaries whose host supervisors determine that they must calculate stand-alone capital requirements (see SCO10) may not incorporate group-wide diversification benefits in their AMA calculations (eg where an internationally active banking subsidiary is deemed to be significant, the banking subsidiary may incorporate the diversification benefits of its own operations — those arising at the sub-consolidated level — but may not incorporate the diversification benefits of the parent).

30.4

The appropriateness of the allocation methodology will be reviewed with consideration given to the stage of development of risk-sensitive allocation techniques and the extent to which it reflects the level of operational risk in the legal entities and across the banking group. Supervisors expect that AMA banking groups will continue efforts to develop increasingly risk-sensitive operational risk allocation techniques, notwithstanding initial approval of techniques based on gross income or other proxies for operational risk.

30.5

Banks adopting the AMA will be required to calculate their capital requirement using this approach as well as the 1988 Accord as outlined in RBC20.14.

General standards for using the AMA

30.6

In order to qualify for use of the AMA a bank must satisfy its supervisor that, at a minimum:

1. Its board of directors and senior management, as appropriate, are actively involved in

the oversight of the operational risk management framework;

2. It has an operational risk management system that is conceptually sound and is implemented with integrity; and
3. It has sufficient resources in the use of the approach in the major business lines as well as the control and audit areas.

30.7

A bank's AMA will be subject to a period of initial monitoring by its supervisor before it can be used for regulatory purposes. This period will allow the supervisor to determine whether the approach is credible and appropriate. As discussed below, a bank's internal measurement system must reasonably estimate unexpected losses based on the combined use of internal and relevant external loss data, scenario analysis and bank-specific business environment and internal control factors. The bank's 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.

Qualitative standards for using the AMA

30.8

A bank must meet the following qualitative standards before it is permitted to use an AMA for operational risk capital:

1. The bank must have an independent operational risk management function that is responsible for the design and implementation of the bank's operational risk management framework. The operational risk management function is responsible for codifying firm-level policies and procedures concerning operational risk management and controls; for the design and implementation of the firm's operational risk measurement methodology; for the design and implementation of a risk-reporting system for operational risk; and for developing strategies to identify, measure, monitor and control/mitigate operational risk.
2. The bank's internal operational risk measurement system must be closely integrated into the day-to-day risk management processes of the bank. Its output must be an integral part of the process of monitoring and controlling the bank's operational risk profile. For instance, this information must play a prominent role in risk reporting, management reporting, internal capital allocation, and risk analysis. The bank must have techniques for allocating operational risk capital to major business lines and for creating incentives to improve the management of operational risk throughout the firm.
3. 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.
4. The bank's operational risk management system must be well documented. The bank must have a routine in place for ensuring compliance with a documented set of internal policies, controls and procedures concerning the operational risk management system, which must include policies for the treatment of non-compliance issues.
5. Internal and/or external 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.

6. The validation of the operational risk measurement system by external auditors and/or supervisory authorities must include the following:
    1. Verifying that the internal validation processes are operating in a satisfactory manner; and
    2. Making sure that data flows and processes associated with the risk measurement system are transparent and accessible. In particular, it is necessary that auditors and supervisory authorities are in a position to have easy access, whenever they judge it necessary and under appropriate procedures, to the system's specifications and parameters.

Quantitative standards for using the AMA

30.9

Given the continuing evolution of analytical approaches for operational risk, the Committee is not specifying the approach or distributional assumptions used to generate the operational risk measure for regulatory capital purposes. However, a bank must be able to demonstrate that its approach captures potentially severe "tail" loss events. Whatever approach is used, a bank must demonstrate that its operational risk measure meets a soundness standard comparable to that of the internal ratings-based approach for credit risk (ie comparable to a one year holding period and a 99.9th percentile confidence interval).

30.10

In the development of operational risk measurement and management systems, banks must have and maintain rigorous procedures for operational risk model development and independent model validation.

30.11

The following quantitative standards apply to internally generated operational risk measures for purposes of calculating the regulatory minimum capital requirements.

1. Any internal operational risk measurement system must be consistent with the scope of operational risk defined in OPE10.1 and the loss event types defined in Table 1.
2. Supervisors will require the bank to calculate its regulatory capital requirement as the sum of expected loss (EL) and unexpected loss (UL), unless the bank can demonstrate that it is adequately capturing EL in its internal business practices. That is, to base the minimum regulatory capital requirement on UL alone, the bank must be able to demonstrate to the satisfaction of its national supervisor that it has measured and accounted for its EL exposure.
3. A bank's risk measurement system must be sufficiently 'granular' to capture the major drivers of operational risk affecting the shape of the tail of the loss estimates.
4. Risk measures for different operational risk estimates must be added for purposes of calculating the regulatory minimum capital requirement. However, the bank may be permitted to use internally determined correlations in operational risk losses across individual operational risk estimates, provided it can demonstrate to the satisfaction of the national supervisor that its systems for determining correlations are sound, implemented with integrity, and take into account the uncertainty surrounding any such correlation estimates (particularly in periods of stress). The bank must validate its correlation assumptions using appropriate quantitative and qualitative techniques.
5. Any operational risk measurement system must have certain key features to meet the

supervisory soundness standard set out in this section. These elements must include the use of internal data, relevant external data, scenario analysis and factors reflecting the business environment and internal control systems.

6. A bank needs to have a credible, transparent, well-documented and verifiable approach for weighting these fundamental elements in its overall operational risk measurement system. For example, there may be cases where estimates of the 99.9th percentile confidence interval based primarily on internal and external loss event data would be unreliable for business lines with a heavy-tailed loss distribution and a small number of observed losses. In such cases, scenario analysis, and business environment and control factors, may play a more dominant role in the risk measurement system. Conversely, operational loss event data may play a more dominant role in the risk measurement system for business lines where estimates of the 99.9th percentile confidence interval based primarily on such data are deemed reliable. In all cases, 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.

Detailed loss event type classification — Table 1

Event-type category (Level 1)	Definition	Categories (Level 2)	Activity examples (Level 3)
Internal fraud	Losses due to acts of a type intended to defraud, misappropriate property or circumvent regulations, the law or company policy, excluding diversity/ discrimination events, which involves at least one internal party	Unauthorised activity	Transactions not reported (intentional) Transaction type unauthorised (with 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 takeover / impersonation etc Tax non-compliance / evasion (wilful) 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 (with 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 / discrimination events	Employee relations	Compensation, benefit, termination issues Organised labour activity
		Safe environment	General liability (slip and fall etc) 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 (including fiduciary and suitability requirements), or from the nature or design of a product.	Suitability, disclosure and fiduciary	Fiduciary breaches / guideline violations Suitability / disclosure issues (know-your-customer etc) 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 (unauthorised etc) 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 events	Disasters and other events	Natural disaster losses Human losses from external sources (terrorism, vandalism)

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 Miscellaneous non-client counterparty disputes
		Vendors and suppliers	Outsourcing Vendor disputes

30.12

Banks must track internal loss data according to the criteria set out in [[OPE30.12]] to [[OPE30.15]]. The tracking of internal loss event data is an essential prerequisite to the development and functioning of a credible operational risk measurement system. Internal loss data is crucial for tying a bank’s risk estimates to its actual loss experience. This can be achieved in a number of ways, including using internal loss data as the foundation of empirical risk estimates, as a means of validating the inputs and outputs of the bank’s risk measurement system, or as the link between loss experience and risk management and control decisions.

30.13

Internal loss data is most relevant when it is clearly linked to a bank’s current business

activities, technological processes and risk management procedures. Therefore, a bank must have 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.

30.14

Internally generated operational risk measures used for regulatory capital purposes must be based on a minimum five-year observation period of internal loss data, whether the internal loss data is used directly to build the loss measure or to validate it. When the bank first moves to the AMA, a three-year historical data window is acceptable (this includes the parallel calculations in RBC20.14).

30.15

To qualify for regulatory capital purposes, a bank's internal loss collection processes must meet the following standards:

1. To assist in supervisory validation, a bank must be able to map its historical internal loss data into the relevant level 1 supervisory categories defined in OPE25.16 to OPE25.25 and [[OPE30.11]] and to provide these data to supervisors upon request. It must have documented, objective criteria for allocating losses to the specified business lines and event types. However, it is left to the bank to decide the extent to which it applies these categorisations in its internal operational risk measurement system.
2. A bank's internal loss data must be comprehensive in that it captures all material activities and exposures from all appropriate sub-systems and geographic locations. 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 have an appropriate de minimis gross loss threshold for internal loss data collection, for example €10,000. The appropriate threshold may vary somewhat between banks, and within a bank across business lines and/or event types. However, particular thresholds should be broadly consistent with those used by peer banks.
3. Aside from information on gross loss amounts, a bank should collect information about the date of the event, 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.
4. A bank must develop specific criteria for assigning loss data arising from an event in a centralised function (eg an information technology department) or an activity that spans more than one business line, as well as from related events over time.
5. Operational risk losses that are related to credit risk and have historically been included in banks' credit risk databases (eg collateral management failures) will continue to be treated as credit risk for the purposes of calculating minimum regulatory capital under this Framework. Therefore, such losses will not be subject to the operational risk capital requirements. Nevertheless, for the purposes of internal operational risk management, banks must identify all material operational risk losses consistent with the scope of the definition of operational risk (as set out in OPE10.1 and the loss event types outlined in [[OPE30.11]]), including those related to credit risk. Such material operational risk-related credit risk losses should be flagged separately within a bank's internal operational risk database. The materiality of these losses may vary between banks, and within a bank across business lines and/or event types. Materiality thresholds should be broadly consistent with those used by peer banks.
6. Operational risk losses that are related to market risk are treated as operational risk for the purposes of calculating minimum regulatory capital under this Framework and will

therefore be subject to the operational risk capital requirements.

30.16

A bank's operational risk measurement system must use relevant external data (either public data and/or pooled industry 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 (eg scaling, qualitative adjustments, or informing the development of improved scenario analysis). The conditions and practices for external data use must be regularly reviewed, documented, and subject to periodic independent review.

30.17

A bank must use scenario analysis of expert opinion in conjunction with external data to evaluate its exposure to high-severity events. This approach draws on the knowledge of experienced business managers and risk management experts to derive reasoned assessments of plausible severe losses. For instance, these expert assessments could be expressed as parameters of an assumed statistical loss distribution. 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.

30.18

In addition to using loss data, whether actual or scenario-based, a bank's firm-wide risk assessment methodology must capture key business environment and internal control factors that can change its operational risk profile. These factors will make a bank's risk assessments more forward-looking, more directly reflect the quality of the bank's control and operating environments, help align capital assessments with risk management objectives, and recognise both improvements and deterioration in operational risk profiles in a more immediate fashion. To qualify for regulatory capital purposes, the use of these factors in a bank's risk measurement framework must meet the following standards:

1. 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.
2. 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.
3. The framework and each instance of its application, including the supporting rationale for any adjustments to empirical estimates, must be documented and subject to independent review within the bank and by supervisors.
4. 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 mitigation

30.19

Under the AMA, a bank will be allowed to recognise the risk mitigating impact of insurance in the measures of operational risk used for regulatory minimum capital requirements. The recognition of insurance mitigation will be limited to 20% of the total operational risk capital requirements calculated under the AMA.

30.20

A bank's ability to take advantage of such risk mitigation will depend on compliance with the following criteria:

1. The insurance provider has a minimum claims paying ability rating of A (or equivalent).
2. 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.
3. The insurance policy has a minimum notice period for cancellation of 90 days.
4. The insurance policy has no exclusions or limitations triggered by supervisory 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 supervisory actions.
5. 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.
6. 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.
7. The framework for recognising insurance is well reasoned and documented.
8. The bank discloses a description of its use of insurance for the purpose of mitigating operational risk.

30.21

A bank's methodology for recognising insurance under the AMA also needs to capture the following elements through appropriate discounts or haircuts in the amount of insurance recognition:

1. The residual term of a policy, where less than one year, as noted above;
2. A policy's cancellation terms, where less than one year; and
3. The uncertainty of payment as well as mismatches in coverage of insurance policies.

Calculation of risk-weighted assets

30.22

The risk-weighted assets for operational risk under the AMA are determined by multiplying the capital requirements calculated as set out in this chapter by 12.5.