AMA [1] FILE FOR CALCULATING THE MINIMUM CAPITAL REQUIREMENTS FOR OPERATIONAL RISK

Banking groups that wish to use the advanced measurement approaches (AMA) in their calculation of the minimum capital requirements for operational risk under the new Capital Standards Framework (Basel II) must participate in the validation processes established by the Banco de España. To participate in the said processes, the group's parent entity will have to forward the information included in this file to the Directorate General Banking Supervision[2].

The information contained herein aims to make known the level of compliance with the minimum requirements established by Basel II for the use of AMA approaches and to determine whether institutions will be able to meet these requirements.

Institutions must have their systems prepared for the standard approach, so that they can apply it if the Banco de España does not accept the proposed AMA approach submitted to it.

Furthermore, institutions will also have to be prepared to make capital requirements calculations in accordance with the standard approach for the exposures that are not to be initially included in the AMA approach either because the roll-out plan provides for their inclusion at a later stage or for reasons of immateriality[3].

The following considerations should be taken into account when filling in the information detailed below with respect to the AMA approach:

1. One AMA file should be completed for the whole of the scope covered by the model. However, if within the proposed scope more than one internal operational risk model has been developed (either for different institutions in the group or for different risk categories in a given institution), the relevant sections should be duplicated for the purpose of filling in the required information for each of the models.

2. Additionally, an internal audit plan and a specific internal audit report, the minimum scope of which is detailed in the Annex, should also be included. This report should be updated biannually and forwarded to the Banco de España until it approves the proposed approach.

3. For those exposures initially treated under the standard approach, and which in the future will be treated under advanced approaches according to the roll-out plan submitted, a new updated version of the AMA File, and the required internal audit reports, shall be sent to the Banco de España at least six months before the planned date of implementation of the advanced approaches. The frequency of the audit reports will be biannual, until the Banco de España approves the proposed approach.

4. In the information submitted a clear distinction should be made between the institution's situation when the documentation is submitted and its plans to improve the model in the future.

[1] *Advanced measurement approaches*.
[2] For institutions which are subsidiaries of foreign banking groups not subject to the EU Directive, the subsidiaries themselves or, where applicable, the Spanish institution responsible for consolidation in Spain will forward this information to the Bank of Spain.
[3] The grounds must be explained to the Banco de España.

5. Any additional information to that mentioned in this document that the institution considers relevant for assessing compliance with the minimum requirements for the application of the AMA approach should also be provided.

6. Information should be submitted in electronic format. If certain information required in this file has already been made available to the Directorate General Banking Supervision and is fully up to date, it may be included by reference without re-submitting it.

INDEX:

A. Scope of application

1. Organisational chart of the group. Identification of the legal entities composing it, with specification of their activity, reporting lines and relative importance in terms of total assets, gross income, annual results and number of employees.

2. Scope of application of the internal model for managing operational risk with specification of the operational risk management tools implemented in each legal entity.

   List of legal entities and/or units included in the advanced measurement system. For the entities not included, in which the standardised approach is intended to be used, the following should be specified:

   a. reason for applying this approach
   b. whether this approach is going to be applied temporarily or indefinitely. If temporary: detailed roll-out plan; if indefinite: demonstration of non-materiality.

3. Support for the affirmation that the legal entities included in the internal model for capital calculation are effectively covered by the operational risk management tools. For each legal entity the following should be specified:

   a. The units, areas or departments included in each risk assessment and their relative importance within the legal entity in terms of operational risk (expressed using gross income or, if not sufficiently indicative, another quantity or quantities)
   b. The units, areas or departments in which qualitative management tools are not used, indicating why not.

B. Self-assessment

4. Assessment of the current degree of compliance with the minimum qualitative and quantitative requirements for the chosen approach, indicating the weaknesses identified in the model and the timetable for remedying them.

5. Details and implementation timetable of upcoming changes and future development of the model.

C. Organisational structure

6. Description and documentary support of the role of the board of directors and senior management in the approval and periodic review of the management framework.

7. Composition and functions of the areas, departments and committees involved in the management, measurement and control of operational risk, including, for the committees, the frequency of their meetings and the date when they were set up.

8. Identification, reporting structure and composition of the unit responsible for internal validation.

9. Composition and functions of the committees that, although not directly managing organisational risk, may be related to it.

D. Risk management tools

10. Qualitative risk self-assessment exercises and, if applicable, controls conducted and timetable of upcoming exercises.

11. List and brief description of risk mitigation plans and recommendations effectively implemented and of those anticipated.

12. List and brief description of risk indicators implemented and implementation timetable.

13. Map of top-level processes of the institution.

14. List of contingency and business continuity plans of the institution.

E. Reporting structure

15. List of regular and ad-hoc reports to business and support lines and, in particular, to senior management. Identification of the users of this information and degree to which its preparation has been automated. Content and frequency of these reports.

F. Documentation

16. Corporate manuals on operational risk policies and procedures. Operational risk methodology and corporate tools manuals and internal validation manual. List of when they were last updated, of those responsible for their preparation and of the dates when and bodies to which they were submitted for approval.

17. List of other internal documents considered significant with a brief description of their content.

G. Internal loss event database

18. Operational risk classification criteria:

    a. Definition and description of internal business lines and mapping to the business lines established in the new solvency rules.
    b. Definition and description of event types and mapping to those established in the new solvency rules

19. Internal loss database file

20. Description of:

    a. Those responsible for data input, maintenance and validation of databases.
    b. Automatic and manual procedures for capturing data.

21. Data quality and integrity controls carried out by the operational risk unit. Results of the latest tests performed.

22. Database analysis reports. Historical evolution and distribution of events by unit, business line, and event type. Explanation of changes in and distribution of data.

23. Internal chart of accounts. List of accounts that fully or partially reflect operational risk.

24. Documentation of the 50 main operational loss events net of recoveries (except insurance).

25. Record of significant events considered to be strategic or business risks and therefore excluded from the internal operational risk database.

H. Scenarios

26. Operational risk scenario database.

27. Description of internal procedures for building scenarios

28. Scenario quality control procedures carried out by the operational risk unit. Results of the latest tests performed.

I. Risk mitigation

29. List of insurance policies or other risk transfer mechanisms used for the purposes of capital quantification

30. For every insurance policy or other risk transfer contract:

    a. Evidence of compliance with the minimum requirements established in the new solvency rules.
    b. Calculation of effective insurance coverage in respect of past insured events.

J. Operational risk quantification

31. Complete and detailed description of the methodology used for the quantification of risk, including at least:

    a. Exploratory data analyses performed in order to determine the operational risk categories used for risk quantification and for the verification, where necessary, of the assumptions made in the model.
    b. Methodologies for the use and combination of internal data, external data, scenarios and factors reflecting the business environment and internal control factors.
    c. Methodologies used to estimate the probability functions and analyses applied to select the probability functions to be employed.
    d. Methodology used to estimate the aggregate loss output for calculating regulatory capital.
    e. Methodology of the correlated capital calculation.
    f. Description of the use of risk mitigation techniques in risk quantification.
    g. Analysis performed in order to evaluate the sensitivity and accuracy of capital estimates.
    h. Consideration of diversification effects and methods of allocating capital among the legal entities in the group.

    The following should be specified: the hypotheses and assumptions of the risk measurement system that primarily determine the capital estimate; the stages at which the risk analyst has exercised discretion and the main limitations of the methodology.

32. Database files of internal and external losses, scenarios and business environment and internal control factors used in model quantification. Preliminary processes employed

in order to use this data (internal/external and scenarios) in operational risk quantification should be specified.

33. Results of the calculation process and capital estimate in all stages of the process. These will include at least:

    a. Results of the exploratory data analysis performed to assess the quality and behaviour of the various information sources, rationale for the operational risk categories and verification, where applicable, of the assumptions made in the model.
    b. Comparison of the internal data, external data and scenarios within each operational risk category and the results of the analyses performed to support the methodology chosen for their use and combination.
    c. Results of all the probability adjusted functions and details of the analyses performed to evaluate the reasonableness and quality of the adjustments. The probability functions finally used in each calculation category are to be stated.
    d. Capital and expected loss estimates. A step-by-step assessment of the impact of using the different information sources (internal data, external data, scenarios) and of the effect of the business environment and internal control factors should be performed.
    e. Correlated capital calculation, if applicable.
    f. Capital after use of risk mitigation techniques, if applicable.
    g. Results of analyses of the sensitivity and accuracy of capital estimates.
    h. Results of diversification effects and capital allocation among the legal entities in the group.

34. Calculation and allocation of economic capital for management purposes and , if applicable, reasoned explanation of the differences from regulatory capital.

35. Capital calculation under the standardised approach

K. Technological support of the model

36. Description of technological support, information systems and application packages enabling effective use of databases, management tools and risk quantification procedures.

37. Description of the internal procedures and controls established to ensure the consistency and reliability of the different sources of information relating to the model, indicating those responsible for these controls and their periodicity.

38. Description and application, where appropriate, of contingency plans.

L. Model validation

39. Description of the role of internal validation. Reports submitted.

40. Description of other possible internal controls used to guarantee the consistency of the model. Identification of the units responsible and their functions.

41. List of independent reviews or assistance (external audit, consultancy, etc), including their objectives and the conclusions reached.

ANNEX

Specific internal audit report on advanced models (AMA) for calculating the minimum capital requirements for operational risk

Audit plan

Internal audit has to develop a plan for ongoing review of the group's operational risk management framework and of the operations of the unit specialised in operational risk management and measurement.

This plan should cover all significant activities exposing the group to substantial operational risk. Also, it should be updated regularly to take account of:

- The development of internal procedures for the identification, measurement, monitoring, control and mitigation of operational risk
- The implementation of new products, procedures and systems exposing the group to significant operational risk

Internal audit report

Internal audit should issue a **specific report for the internal operational risk model** in which it explicitly pronounces on at least the matters listed below and documents all its conclusions. It should also include a list of the audit tests performed to support each of the opinions issued.

If an opinion cannot be issued on any of the matters mentioned above because they are not at a sufficiently advanced stage, the implementation timetable and, subsequently, the degree of compliance with it will be indicated.

A. Integration of the measurement system in the management process

Internal audit should verify that the internal operational risk measurement system is integrated in the day-to-day management procedures for this risk. In particular, the various uses of the AMA model additional to its regulatory use should be specified.

Also, the adaptation and evolution of the AMA model as the group acquires more experience in operational risk management techniques should be verified.

B. Operational risk management procedures and tools

Internal audit will have to verify compliance with internal rules on this risk. In particular, it should check that:

1. The internal documentation is complete.
2. The management information reporting procedures are followed.
3. Operational risk assessment and quantification meet the required standards.
4. Monitoring actions are effective and timely.

5. The procedures for reviewing and updating the operational risk management framework are followed.
6. The risk indicators/loss data/compliance reports and risk estimates are in line with the results of the qualitative self-assessment.

C. Operational risk measurement system

Internal audit should take into account the specific purpose for which the operational risk management system is used, including all quantitative and qualitative elements, as follows:

1. All the elements that are to form the operational risk measurement system in an AMA model should be verified to ensure that they are understandable, appropriate and accurate and that they comply with the group's internal rules and the standards applicable to this risk class:
    a. Internal data. It should be verified that the information captured:
        i. is full and complete
        ii. is consistent throughout the whole organisation
        iii. is suitable for calculating regulatory capital
        iv. results from application of the internal policies on:
            iv.a. identification of the events that will form part of the regulatory capital calculation database.
            iv.b. treatment of the possible gains arising from the events
            iv.c. treatment of multiple losses (incurred in different time periods or affecting different units)
            iv.d. setting of minimum thresholds for capture of losses in the different operational risk categories defined by the group.
    b. External data.
    c. Scenario analysis.
    d. Business environment and internal control factors.
2. If any of the above four elements, which should form the operational risk measurement system, contain qualitative data, Internal audit will have to check that these data are appropriate for accurately defining the risk factors.
3. It should be checked that the relationship between model inputs and outputs follows the procedure established by the group and that this procedure is transparent and consistent.

D. Technological environment and computer applications

The activity of Internal audit should also include matters such as the suitability of technological infrastructures and data capture and maintenance, in order to check that the model is used effectively. In particular the following should be checked:

1. The degree of internal integration (between model components) and external integration (with other information systems in the institution), identifying manual procedures, technological weaknesses and possible deficiencies in other external systems that may affect the model.

2. Regarding computer applications:
    a. Availability of data and replicability of databases used in the model over time.
    b. Degree of automation of periodic processes for the proposed regulatory use.
    c. Suitable programming of the calculation methodologies used in the model.
    d. *Replicability* of model outputs.
3. Regarding the model as an information system:
    a. *Maintenance* processes.
    b. Systems plan.
    c. Database management.
    d. Contingency plans.
    e. Adequacy of *resources (*human, software and hardware*)*.

4. Existing technical documentation.