GUIDELINES ON ASSESSMENT, VALIDATION AND CORPORATE GOVERNANCE OF INTERNAL RATING BASED APPROACHES AND ADVANCED MEASUREMENT APPROACH

I. OBJECTIVE AND SCOPE

1. The objective of these guidelines is to assess the approaches used within the scope of Communiqué on Calculation of the Risk Weighted Exposure Amount for Credit Risk by Internal rating based Approaches (IRB Communiqué) published in the Official Gazette dated October 23, 2015 number 29511 and Communiqué on Calculation of the Risk Weighted Exposure Amount for Operational Risk by Advanced Measurement Approach (AMA Communiqué) published in the Official Gazette dated September 6, 2014 number 29111 and to explain minimum rules and principles on validation.

2. The Agency may ask for more rigid or detailed implementations than those stated in these guidelines. In such a case, no banks can avoid to implement the additional conditions asked by the Agency simply because they are not included within the scope of these guidelines.

3. In these guidelines, no differentiation is made between "Basic IRB Approach" and "advanced IRB Approach". Therefore, the best practices stated in these guidelines are expected to be implemented at the same level for both approaches.

4. The operational structure to be implemented by banks within the scope of validation of IRB models is expected to be composed of three main elements. The first one is Credit risk control unit[1] (CRCU) to be implemented pursuant to Article 4(2c) of the IRB Communiqué. Pursuant to IRB Communiqué, Annex-2, Paragraph 64, the mentioned unit is responsible for the design or selection, implementation, oversight and performance of rating system, regular analysis to be made on the results and reporting the results of analysis to the senior management at least twice annually. This unit shall be the owner of IRB models in the bank ("owner" here means, concerning the mentioned models, it will be the main respondent of the Agency, independent from whether or not CRCU developed the model or models). The mentioned unit is expected to operate under risk management unit. In addition, pursuant to IRB Communiqué, Annex-2,

[1] The unit to be established pursuant to IRB Communiqué, Article 4(2c).

paragraph 57, the validation is expected to be made, at least once annually, by a unit[2] independent from the personnel responsible for design and selection as well as implementation of the model or by an independent third party. In other words, it is required to establish a validation unit independent from CRCU and executive units or the validation should be made by an independent third party. Finally, pursuant to IRB Communiqué, Annex-2, paragraph 67, internal audit unit of the bank should be responsible for regular review and inspection of the activities of CRCU and validation unit (including the validation to be made by independent third parties).

5. In these guidelines, best practices on the below-mentioned issues are explained;

   a) Concerning quantitative and qualitative validation;

      - Principles on validation,
      - Validation instruments,
      - Low-default portfolios,
      - Internal validation of operational risk measurement and management processes,

   b) Concerning corporate governance;

      - Issues within the scope of IRB Communiqué,
      - Issues within the scope of AMA Communiqué,
      - Role of board of directors and senior management,
      - Risk management organization,
      - Role of internal audit,
      - Independence/conflict of interests in rating systems,
      - Role of external auditors in the review process.

II. DEFINITIONS

6. Following terms used in these guidelines shall have the meanings designated to them;

   a) Benchmarking: means the process of comparing the consistency of estimated parameters with those obtained by using other estimation techniques (for example, other rating

[2] The team stated in IRB Communiqué, Annex-2, Paragraph 57.

systems) and /or assessing them by using other potential data resources (for example, other banks or credit rating institutions),

b) Credit spread: Premium above government or risk-free rate, required by the market for taking on credit exposures,

c) Override: means changing, by judicial intervention, downward or upward the rating grade obtained by a model,

d) Validation: means determination of in which ratio the models used within the scope of methodology represents the realizations by using certainty, accuracy and consistency criteria and evaluation of the soundness of other aspects of the methodology.

III. QUANTITATIVE AND QUALITATIVE VALIDATION

III.1. Principles on Validation

7. In this section, principles on validation process is set forth.

8. Rating systems and outputs of those systems are used by banks for many different purposes. As a general rule, validation made by banks should consider the usage purpose of rating systems and the model changes made in this direction (without prejudice to the general conditions concerning the usage test which requires the explanation of reasons of the differences between measurements used for legal risk parameters and internal purposes).

9. The IRB framework requires banks to assess the ability of a borrower to perform in adverse economic conditions. Thus, when considering the appropriateness of any rating system as the basis for determining capital, there will always be a need to ensure objectivity, accuracy, stability, and an appropriate level of conservatism.

10. Internal ratings and default and loss estimates must play an essential role in the credit approval, risk management, internal capital allocation, and corporate governance functions of banks using the IRB approach. The IRB Communiqué recognizes that the management of banks continues to bear responsibility for validating the inputs to the IRB approach. Agency has the responsibility for assessing the compliance of banks' validation of their rating systems and inputs with the IRB framework's minimum standards. Agency must ensure that these requirements are met, both as qualifying criteria and on a continuing basis. Validation is thus a fundamental aspect of the IRB approach and explained in the principles below.

Principle 1: Validation is fundamentally about assessing the predictive ability of an institution's risk estimates and the use of ratings in credit processes.

11. A bank's IRB estimates are intended to be predictive. While grounded in historical experience, they should also be forward-looking. Rating systems should effectively discriminate risk (i.e., credits with lower ratings should have a higher risk of loss) and calibrate risk (i.e., they should accurately quantify the risk of loss). Rating systems should also be consistent. If the processes that are used in assigning risk estimates are not accurate, then the risk estimates may fail to be sufficiently predictive and may under or overstate required regulatory capital. Consequently, validation should focus on assessing the forward-looking accuracy of the bank's risk estimates, the processes for assigning those estimates, and the oversight and control procedures that are in place to ensure that the forward-looking accuracy of these estimates is preserved going forward. As a general rule, the validation process should prompt a reassessment of the IRB parameters when actual outcomes diverge materially from expected results. In order to ensure the predictive accuracy of its risk estimates as well as the effective discrimination and calibration of risk, a bank will first need to assess the general appropriateness of each of its rating systems.

    This assessment will cover at least:

- Verification that each rating system is characterized by an appropriate balance of objectivity, accuracy, stability and conservatism.
    - Objectivity requires the adoption of policies and standards that ensure that ratings and estimates are applied consistently to borrowers and facilities with similar characteristics and posing similar levels of risk. Judgment is a necessary part of any overall rating system. It plays an important role in the development of the system and in the assignment of individual ratings and estimates, including overrides. However, banks must be able to verify how the use of judgment is managed in order to achieve consistent outcomes. For the purposes of comparing outcomes against expected performance, banks should be able to identify how their estimates have been adjusted from the most likely outcome.
    - Accuracy requires the adoption of policies and standards relating to the expected performance of the rating system (outcomes versus predictions) and to the integrity of inputs into the rating system and their conversion into outputs.

- Stability requires the adoption of policies and standards that ensure that ratings and estimates are broadly unchanged when the underlying risk has not changed. This should not preclude changes that are intrinsic to the rating philosophy of the system.
- Conservatism requires the adoption of polices and standards that identify the sources and range of uncertainty in ratings and estimates, and the degree of conservatism. In particular, the policies should identify where and explain how the bank applies conservatism in accordance with the relevant requirements of the IRB Communiqué.

- The appropriateness of the philosophy of each rating system.
  - The philosophy of a rating system can be characterized by two components: the philosophy underlying the grade or pool assignment (i.e.: how banks assign exposures, obligors or facilities to 'risk buckets' (according to appropriate risk drivers)) and the method used to quantify the risk parameters associated with each grade or pool.
  - The IRB Communiqué does not prescribe the philosophy that must underlie the grade or pool assignment in a rating system. Each philosophy results in a specific dynamics of ratings. The philosophy underlying the grade or pool assignment could be characterized by the extent to which a change in economic conditions is expected to result in a net migration of a large number of exposures, borrowers, or facilities to other grades or pools (if the bank were to take no compensating policy actions), as opposed to migration of some exposures, borrowers, or facilities to other grades or pools due only to their individual characteristics while leaving the number of exposures, borrowers or facilities in each grades or pools substantially unchanged, or a hybrid between these two extremes.

12. In order to assess the appropriateness of the philosophy of a rating system, the bank should:

- Understand the philosophy underlying the grade or pool assignment, and specifically the risk drivers, and whether they create homogeneous buckets with respect to the targeted estimator.
- Assess whether the method used to quantify the risk parameter is adequate for the philosophy underlying the grade or pool assignment.
- Understand the characteristics, including the dynamics, of its ratings and of its risk parameter estimates (i.e.: whether the PD estimates are derived from point in time ratings or through the cycle ratings).

- Assess the adequacy of the resulting characteristics, including the dynamics, of the ratings and risk parameter estimates with regard to their different uses.
- Understand the impact of the characteristics, including the dynamics, of the ratings and risk parameters estimates on the dynamics and volatility of capital requirements.

13. The bank should at least adopt and document policies which explain the philosophy of each rating system and how grades and risk parameters are expected to vary with movements in the general economic cycle or more specific cycles relevant to each risk parameter. These should include descriptions of how, if at all, rating assignments and risk parameter estimates are impacted by the application of conservatism.

14. When a bank uses different rating systems characterized by different philosophies, care should be taken in the use of information, either for rating assignments or estimates, from another (internal or external) rating system that has a different rating philosophy. An example is the use of rating information or default experience obtained from rating agencies. When a bank uses different rating systems with different characteristics (for example, different philosophies, levels of objectivity, accuracy, stability, or conservatism) it should ensure that they have an appropriate level of consistency and/or that the differences between them are well understood. This understanding should at least enable the bank to define an appropriate way to combine/aggregate the information produced by the different rating systems when this is necessary. The assumptions and potential inaccuracies arising from such a combination/aggregation should be fully understood.

15. For example, the bank should at least describe how the combination of information from rating systems characterized by different philosophies impacts the dynamics and volatility of capital requirements.

16. Historical data are an important source of information for constructing estimates of future default frequencies and losses, but they are only a starting point and should be adjusted with care. The minimum data periods (five or seven years) in IRB Communiqué determine how much (minimum) historical experience is needed as an input to the forward-looking estimates, and are not meant to imply that an average of actual experience is a sufficient measure for the forward-looking estimates. Nevertheless, where a bank can demonstrate that the historical experience is likely to be an accurate estimate of the forward-looking estimate, little or no adjustment may be needed.

17. Forward-looking estimates can be lower than actual historical experience. This may be because of small sample size, because the historical experience contains a disproportionate number of extremely bad years, or because practices have changed. However, a high burden of proof would be placed on any bank that sought to ignore or significantly underweight some of the available data.

18. PD estimates must be based on the long run average of default rates in each grade or pool. This implies that the historical experience needs to include a representative mix of good and bad years for the economy as a whole, as well as addressing more specific (e.g., industry) cycles that are material to the level and volatility of defaults in exposures covered by the rating system. Banks must demonstrate that the estimates they are using are representative of likely long run rates. Where (internal or external) statistical prediction models are used, this may require an adjustment to the calibration of those models.

19. Similar considerations apply to estimates of LGD and CF based on default weighted averages. These averages will naturally be oriented towards the losses expected to be incurred (or the appropriate CF) under conditions when defaults for the exposures in question are expected to be high, as opposed to more normal market conditions. This should encourage more stable estimates, although banks should ensure that those estimates are at least conservative enough to represent economic downturn conditions (if this is more conservative than the long run average).

20. Banks should have policies and standards covering the levels of accuracy and, where relevant, discriminative power, the acceptable levels of divergence from the expected performance, and the action to be taken when these acceptable levels are breached. They should also have clear policies for the circumstances in which these standards may be changed.

Principle 2: The credit institution has primary responsibility for validation.

21. Agency do not have the primary responsibility for validating banks' rating systems. Rather, a bank has the primary role, and consequently must validate its own rating systems to demonstrate how it arrived at its risk estimates and confirm that its processes for assigning risk estimates are likely to work as intended and continue to perform as expected. Agency, on the other hand, should assess the bank’s validation processes and outcomes and may rely upon additional processes of its own design, or even those of third parties, in order to have the required level of supervisory comfort or assurance.

Principle 3: Validation is an iterative process.

22. Validation is likely to be an ongoing, iterative process in which banks and Agency periodically refine validation tools in response to changing market and operating conditions. Banks and Agency will need to engage in an iterative dialogue on the strengths and weaknesses of particular rating systems. Banks will need to adjust and improve their validation techniques in response to changing practices in the industry and as more data becomes available.

Principle 4: There is no single validation method.

23. While some validation tools (e.g., back testing, benchmarking, replication, etc.) may prove especially useful, there is no universal quantitative or qualitative tool that can be used for all portfolios in all banks. Back testing, for example, may prove difficult for portfolios where there is a low level of historical defaults. Validation techniques may converge over time, but in practice there will likely be differences in validation techniques across portfolios (e.g., retail vs. corporate credit) and across markets. In addition, the underlying philosophy of the rating system must be well understood and properly taken into account when determining which validation tools and techniques should be applied. This applies both to the choice of validation methods for assessing the accuracy and stability of a rating system, and to the choice of methods for assessing the appropriateness of the stress tests applied to that system.

- A validation process needs to contain a mix of developmental evidence (assessing the logic of the approach, its conceptual soundness, statistical testing performed prior to use), benchmarking and process verification (comparisons to relevant alternatives, verification that the process is being applied as intended), and outcomes analysis (back testing).
- The balance in the required use of these tools will vary between rating systems, depending for example on the extent to which outcomes analysis is reliable.

Principle 5: Validation shall comprise both quantitative and qualitative aspects.

24. While validation can be thought of as a purely technical/ mathematical exercise in which outcomes are compared to estimates using statistical techniques, focusing solely on comparisons between predictions and outcomes is likely to be insufficient. In assessing the overall performance of a rating system, it is also important to assess the components of the rating system (data, models, etc.) as well as the structures and processes underlying the rating system. This should include an assessment of controls (including independence), documentation, internal use, and other relevant qualitative factors.

- Outcomes analysis is not a sufficient technique for validating all or part of a rating system. To the extent that outcomes analysis does provide strong support for the estimates, there

will be less need to rely on other elements. However, even in these cases, banks should focus on the possibility of future changes in the economic environment, borrower composition, the bank's practices, etc., which result in those estimates no longer proving valid in the future. Where outcomes analysis is less reliable, more emphasis will need to be placed on how the rating system is implemented and used in practice, the reasonableness of other validation procedures used and how they are monitored, and the existence of an appropriate control and technology environment.

- Banks should be able to bring sufficient experience and judgment to the development, adjustment, interpretation, and validation of rating systems and estimates, to supplement purely quantitative techniques.
- The qualitative phase of the bank's assessment should focus on how the various information is interpreted to produce final assignments of the grades or pools and parameter estimates.

Principle 6: Validation processes and outcomes should be subject to independent review.

25. It is important that a bank's validation processes and results should be reviewed for integrity by parties within its organization that are independent of those responsible for the design and implementation of the validation process. This independent review of validation is of the responsibility of Internal Audit unit. Support can be taken from independent units (independent from CRCU and executive units) and/or independent third parties.

III.2. Validation tools concerning IRB approach: Benchmarking and Back testing

26. IRB Communiqué, Annex-2, paragraph 57 (a) requires the bank's estimation to be accurate and consistent, (b) and (c) requires regular back testing and benchmarking of their IRB risk quantification for each grade, (ç) ensuring the consistency of methods and data through time and documenting changes in methods and data (d) taking account of unexpected changes in economic conditions. The following part of these guidelines elaborates on these requirements and fleshes out general principles 4 and 5 discussed above.

27. Banks are expected to provide sound, robust, and accurate predictive and forward-looking estimates of risk parameters (PD, LGD and CF). They shall have a system of risk segmentation which accurately differentiates risk, and a quantification process which accurately estimates those parameters. The bank's validation process has to ensure that these requirements are met on an ongoing basis.

28. Common quantitative validation tools include back testing and benchmarking of the internal rating system outputs. The IRB Communiqué explicitly requires banks to use both tools in their

validation process (Annex-2, sub-paragraphs (b) and (c) of paragraph 56). Back testing consists of checking the performance of the risk rating systems estimates by comparing realized risk parameters with estimated risk parameters. Benchmarking consists of comparing the outputs of the reviewed risk rating systems with relevant external data sources provided that those data are appropriate to the portfolio (according to Annex-2, sub-paragraph (c) of paragraph 56). In cases where a lack of internal or external data prevents the proper use of these techniques, banks should apply an appropriate margin of conservatism in their estimations. However, if the lack of data is caused by the efforts of the bank to use only data that was collected under economic downturn conditions, the use of an additional layer of conservatism should be carefully assessed.

III.2.1. Back testing against rating systems

29. Back testing generally involves comparing realized (expost) values with estimated (exante) parameters for a comparable and homogeneous data set (for example, comparing realized default frequencies with estimated PDs).

30. Back testing is expected to compare realized default rates, loss severities, and exposure at default experience in each rating grade with the PD, LGD, and CF values that have been estimated using an internal IRB model. This can be accomplished by using statistical methods to implement statistical tests for defining acceptable levels of the potential discrepancy between exante expectations and expost realizations.

31. At a minimum, the assessment of back testing results should focus on the following issues:

    - The underlying rating philosophy used in developing rating systems (e.g., are PDs derived from point in time or through the cycle ratings?). Banks that use different rating systems will need to take into account any differences in their rating philosophies when back testing estimates of risk parameters. Failing to do so would lead to erroneously assigning differences in rating philosophies to inaccuracies in reported estimates.
    - Banks should have policies that outlines remedial actions, for example, whenever back testing results breach internal tolerance thresholds for validation, if such thresholds are used.
    - When back testing is hindered by lack of data or insufficient quantitative information, banks will need to rely more heavily on additional qualitative elements such as quality control tests, benchmarking with external information, etc. This might be particularly relevant in the case of estimates that relate to rarely observed economic downturn conditions.

- The identification of the specific reasons for discrepancies between predicted values and observed outcomes (e.g., variations through time that might affect banks' risk analysis and consequently their back testing results).
- Banks should adopt and document policies which explain the objectives and logic underlying their back testing exercises.

III.2.2. Benchmarking the outputs of internal ratings systems against external data

32. Benchmarking involves assessing the consistency of the estimated parameters with those obtained by other estimation techniques (such as other rating systems), or potentially using other data sources (such as other banks or ECAIs). It helps to assess whether banks have quantified the risk parameters accurately by comparing them with a set of 'reference data' consisting of alternative PD, LGD and CF estimates from internal and external sources.

33. When performing benchmarking risk estimates against other sources, banks should investigate the sources of substantial discrepancies between the values of risk parameters resulting from their internal risk rating system and those obtained from the other sources.

34. Regardless of the benchmarking method used, banks shall demonstrate to the Agency that their rating systems are performing in compliance with the minimum requirements in Annex-2 of the IRB Communiqué.

35. In the assessment of benchmarking results, specifically, banks should consider the followings:

- The underlying rating philosophy used in developing rating systems (e.g., are PDs derived from point in time or through the cycle ratings?). Banks that use different rating systems will need to take into account any differences in their rating philosophies when back testing estimates of risk parameters. Failing to do so would lead to erroneously assigning differences in rating philosophies to inaccuracies in reported estimates;
- The procedure for establishing tolerance thresholds for validation, and the list (at least in broad terms) of the types of possible responses when thresholds are breached;
- The additional qualitative elements of their implementation of benchmarking;
- The identification of unanticipated changes over time that might affect benchmarking results;
- Banks should adopt and document policies which explain the objectives and logic underlying their benchmarking exercises.

III.3. Low-default portfolios

36. The IRB applies certain conditions to PD estimations (for example, the bank must estimate long run, forward looking expected default rates for each rating grade, with an appropriate margin of conservatism). Certain conditions also apply to their validation. Nevertheless, there can be portfolios with a low number of defaults due to the lack of sufficient default or loss data to satisfy the IRB Communiqué requirements for validation.

37. Low default portfolios are portfolios with few or no defaults observed. Low default portfolios can arise under different circumstances, and can be categorized as follows:

    - Long term, due to high quality borrowers (e.g., banks) or a small number of borrowers (e.g., sovereigns), versus short term (e.g., new entrants into a market); or
    - Systemic (data unavailable for all banks), versus bank specific (data unavailable for the bank in question, perhaps due to insufficient effort to enhance its database with suitable external data).

38. The following principles are aimed at systemic low default portfolios, and do not generally apply to bank specific low default portfolios.

39. Exposures in low default portfolios should not necessarily be excluded from the IRB approach simply because of the absence of sufficient data to validate PD, LGD and CF estimates on a statistical basis. Such exposures may be included if banks can demonstrate that the methods and techniques applied to estimate and validate PD, LGD and CF constitute a sound and effective risk management process and are employed in a consistent way. Banks will be required to use appropriate conservatism in risk parameter estimation.

40. The bank's process for estimating PD, LGD, and CF in low default portfolios should be supported by appropriate methodologies. Even in the absence of defaults, additional information (ratings, prices, etc.) might be available that can be used in the estimation process. Wherever possible, banks should take such additional information into account in their estimation process. The validation process for low default portfolios should not be completely different from the validation process for non-low default portfolios, and banks should ensure compliance with the minimum requirements laid down in IRB Communiqué applicable regulations, in particular regarding adequate margins of conservatism.

41. Banks should pay particular attention to implementation and use, and to ensuring that control and technology environments and internal validation procedures are appropriate.

42. Banks should reinforce qualitative validation of low default portfolios, relative to non-low default portfolios. The design of rating models, the quality of the data used in developing and deploying the model, and the internal use of the rating system should be key areas of the validation process for low default portfolios. A high level of compliance with the use test is an important indicator of a bank's confidence in its estimates, and will therefore be viewed as a necessary part of meeting the minimum requirements. However, meeting the use test is not in itself a sufficient condition, and should in any event be treated with particular caution for low default portfolios, given the inherent difficulty in proving the accuracy of the estimates of PD, LGD, and CF. As is the case with non-low default portfolios, standardized procedures should be applied for assigning ratings in low default portfolios. These procedures can be based on expert judgment and/or on external data. In any case, it is necessary to monitor the quality, objectivity and credibility of the data sources, and to strengthen the transparency and completeness of documentation.

III.3.1. Quantitative Validation

43. Limitations in the dataset should not exempt banks from performing a quantitative validation on low default portfolios. Whenever few or no defaults are observed, a quantitative validation could be approximated (e.g. by assessing rating migrations, using credit spreads where appropriate etc.). Adequate and consistent methods should be used to ensure a sound and effective assessment and measurement of risk. The criteria to be reviewed in quantitative validation should include at least calibration, discriminative power, and stability.

44. The approach for calibration is likely to be based more on expert judgment, utilizing the extensive internal and/or external experience with the particular type of business.

45. Banks could use a variety of quantitative and qualitative analyses to provide confidence in, and an indication of, the discriminative power of the models. Depending on the amount of data, different techniques can be used:

- Internal benchmarking.
- Comparison with other ratings and models.
- Comparison with other external information

III.4. Internal validation of risk measurement and management processes

46. This section examines the scope of AMA internal validation.

47. The following high level principles apply to validation:

- Internal validation is the responsibility of the bank. The bank should make a 'best effort' to internally validate its AMA framework.
- Banks should establish a clear methodology for internal validation. This methodology should be appropriate for the organization and its AMA framework, and should be clearly documented.
- There is no single validation method. Internal validation techniques should be proportionate and take into account changing market and operating conditions.
- Internal validation should encompass both quantitative and qualitative elements.
- Internal validation processes and outcomes should be subject to independent review to ensure that implementation is effective.

48. The frequency of internal validation will ultimately depend on what is being validated and on its significance in the bank's risk measurement systems or risk management processes. Banks should conduct a complete internal validation programme, including independent review of the internal validation processes and outcomes, before submitting the AMA application.

49. Banks should periodically analyze their internal validation methodology to ensure that it remains appropriate. In particular, certain parts of the risk measurement systems and risk management processes should be revalidated, at least if there is a significant change in the bank’s operational risk profile and/or in the model's methodology/assumptions or management processes.

III.4.1. Validation of Risk Measurement Systems

50. Validation of operational risk measurement systems presents major challenges to banks. Nevertheless, a bank has to have an internal validation process. This should be proportionate and should take into account the specific purposes for which the operational risk measurement systems are used.

51. Banks should ensure that information that is feeded into the risk measurement systems is as accurate and complete as reasonably practicable.

52. There are many methods that can be used for validation; and, as banks gain experience, new validation techniques will emerge. A bank should consider a robust approach to validation and should be able to explain and justify its methodology. A bank's internal validation of its risk measurement systems should encompass both quantitative and qualitative elements and be clearly documented. This documentation should provide a detailed outline of the validation methodology (including frequency), and outline any identified weaknesses.

III.4.2. Model input, methodology and output

53. The bank should have clear standards for the input of data into its model, to which it must adhere.

54. All material data above the thresholds set must be validated to ensure that they are comprehensive, appropriate, and accurate. Validation should cover all data types: actual data, constructed data, figures generated by scenario analysis, factors relating to business environments, and internal control factors. Particularly for constructed data, the validation should ensure that the assumptions are unbiased and the results are realistic.

55. The bank should ultimately be able to ensure the validity of the model input on an ongoing basis.

56. Model validation should ensure that the relationship between the inputs and outputs of the model are stable and that the techniques underlying the model are transparent and intuitive. The model should be logical: if controls are improved, then EL and/or UL relating to operational risk should decrease; and hence, all other things remaining equal, there should be a corresponding reduction in regulatory capital.

57. The bank should be able to ensure the validity of the model methodology at the development stage and following significant changes in methodology/assumptions, and it should be able to ensure the validity of the model output on an ongoing basis.

III.4.3. Validation of Risk Management Processes

58. Banks should have robust risk management processes for managing operational risk throughout the business. Banks will be expected, as part of the internal validation process, to assess the appropriateness of their risk management processes. This is to ensure that the framework remains 'fit for purpose' and operates as management would expect it to.

59. Validation of the risk management processes should be an ongoing exercise. Banks should be able to justify to the Agency how they do this. Banks can use a variety of validation techniques. These include verifying that:

    - Risk management documentation is complete.
    - Management information reporting procedures are followed.
    - Captured loss data meet the required data standards.
    - Follow up actions are carried out in an effective and timely manner.
    - Procedures to review and update the operational risk management framework are followed.

- KRI's/loss data/compliance reports and risk estimates are in line with the results of qualitative self-assessments.

IV. CORPORTAE GOVERNANCE

IV.1. Issues within the scope of IRB

60. Annex-2, Paragraphs 60 to 65 the IRB communiqué set out minimum requirements regarding corporate governance and oversight, including a brief description of the roles of the board of directors and senior management. This section of the guidelines elaborates further on those minimum requirements.

61. The aim of this section is not to lay down a 'one-size-fits-all' approach to assessing a bank's organizational structure, corporate governance, and internal control systems. The Agency demand banks to make their assessment according to their characteristics, taking into account their size and the complexity and nature of their business ('the principle of proportionality').

62. Paragraph 63 of the Annex-2 of the IRB Communiqué emphasizes on the activities concerning the management of rating systems and the organization which will conduct these activities. This organization is named CRCU.

63. In the paragraph 63 of the Annex-2 of the IRB Communiqué, it is determined that CRCU is responsible for the design or the selection of rating systems, their implementation, oversight and performance. The mentioned unit should inform senior management regularly about the performance of the rating system, as well as areas needed to be improved and remedial actions about the deficiencies detected

64. For internal validations, a validation unit independent from CRCU and executive units should be established in banks, under the risk management unit and this unit should make periodical reporting to the senior management about validation results. Validations done before the publication of these guidelines that are carried out by independent teams instead of a validation unit will not constitute a problem.

IV.2. Issues within the scope of AMA

65. Operational risk management differs from credit risk management, reflecting fundamental conceptual differences between operational risk and credit risk. Operational risk is inherent in every activity performed by a bank and in every part of its organization, while credit risk is localized in portfolios. Credit risk is actively taken, in order to generate income, while operational risk is inherent in every activity performed by a bank. The amount of credit risk that

a bank wants to take on can be defined and controlled using a limit system, while it is difficult to set limits for operational risk (although it can be mitigated by insurance and/or internal controls).

66. Within the scope of AMA, in particular, with regard to corporate governance matters, the following elements have to be taken into account:

- **Reporting**: There should be a regular reporting on operational risk exposures and loss experience. The bank shall have procedures for taking appropriate corrective action. (AMA Communiqué, Article 5 (1c)).
- **Operational risk management function (ORMF)**: The bank should have an independent risk management function for operational risk. (AMA Communiqué, Article 5 (1b)).
- **Internal Audit:** The operational risk management processes and measurement systems shall be subject to regular reviews performed by internal and/or external auditors (AMA communiqué, Article 5 (1d)).

IV.3. Role of board of directors and senior management

IV.3.1 Responsibility hierarchy

67. In this section, common issues concerning both IRB approaches and AMA as well as the issues peculiar to credit risk or operational risk are explained. Provisions in which it is not clearly stated whether or not it is related to credit risk or operational risk is valid for both risk types.

68. Sound corporate governance requires that the decision making process be clearly stated within each bank, in terms of hierarchy and level of responsibility. In order to improve understanding of the operational risk measurement system among the board of directors, and to improve efficiency, the board of directors may, where appropriate, establish specific Risk Committees and delegate certain aspects of this framework to these committees or to senior management. Senior management itself may also delegate certain tasks. However, such delegations do neither relieve the board of directors and senior management from their obligation to have a general awareness of the IRB/AMA framework used by their bank, nor do they relieve the board of directors from its ultimate responsibility for the IRB /AMA framework and the senior management from its responsibility for developing and implementing it.

69. Both the board of directors and senior management should be responsible for approving all material aspects of the “rating and prediction processes"/"operational risk management frame. They should have a general understanding of the bank’s "rating/ operational risk measurement

systems" and detailed comprehension of its associated management reports submitted to them and how operational risk affects the bank. The material aspects of the overall operational risk framework encompass:

- Activities aimed at identifying, assessing and/or measuring, monitoring, controlling, and mitigating operational risk;
- Risk management strategies and policies concerning IRB/AMA system (including allocation of grades for credit risk and all aspects of risk parameter prediction process);
- The organizational structure of the control functions (ex. internal audit and internal control); and
- Specifying levels of acceptable risk (by using IRB results in the definition of risk profile for credit risk).

70. Both the board of directors and senior management are responsible for making formal decisions on the implementation of the IRB/AMA approach. This includes the overall approval of the project, the specification of goals, and the appointment of the organizational structures responsible for implementation. A time schedule of the necessary steps should be provided with the project approval. Both management functions are responsible for effective management of IRB/AMA frame and below-mentioned issues shall be provided by the mentioned management functions.

71. The board of directors has to exercise effective oversight. Senior management should therefore notify the board of directors, or a designated committee thereof, of material changes or exceptions from established policies that will materially impact the bank's rating systems and operational risk measurement systems and management processes. Board of directors should review on an ongoing basis the control procedures of internal audit unit.

72. The senior management should be involved, on an ongoing basis, in the oversight of the control procedures and measurement systems of CRCU/ORMF and the protection of efficiency of overall IRB/AMA system over time. The senior management should comprehend well the design and functioning of "rating"/"operational risk" system. In addition, concerning credit risk, senior management shall have a good understanding relating to credit policies, credit standards, credit extension as well as follow-up and collection implementations, and comprehend how these factors affect related risk parameters. Senior management should ensure that the following tasks are being addressed:

- Ensuring the soundness of risk taking and risk management processes even under changing conditions rapidly;

- Determining how the internal grades are used in risk taking process for credit risk;
- Informing the board of directors, or a designated committee thereof, of material changes or exceptions from established policies that will materially impact the functioning of "rating systems"/operational risk measurement systems and management processes";
- Identifying and assessing the main risk factors, based on information provided by CRCU/ORMF;
- Defining the tasks of the CRCU/ORMF and evaluating the adequacy of its professional skills;
- Monitoring and managing all sources of potential conflicts of interest;
- Establishing effective communication channels in order to ensure that all staff are aware of relevant policies and procedures;
- Defining the content of reporting to the board of directors or to different delegated committees thereof (e.g., the Risk Committee);
- Examining reports from Internal Audit unit; and
- Adequately assessing operational risk inherent in new areas (products, activities, processes, and systems) before they are introduced, and identifying risks tied to new product development and other significant changes in order to ensure that the risk profiles of product lines are updated regularly.

73. Moreover, senior management shall regularly control whether or not control procedures and measurement systems implemented by CRCU/ORMF and internal audit unit are adequate and efficiency of overall IRB/AMA system maintained efficient over time.

74. CRCU/ORMF designs, develops, implements, and executes risk management and measurement processes and systems. Furthermore, CRCU ensures effective operating of rating systems and submits to the approval the usage of these systems.

75. The Internal Audit should provide an assessment of the overall adequacy of the internal control systems and CRCU for credit risk and operational risk management framework for operational risk.

IV.3.2. Internal Reporting

IV.3.2.1. Issues concerning IRB

76. Internal rating based analysis of the bank's credit risk profile should be an essential part of the internal reporting system. The recipients of the reporting should include not only the board of directors and senior management, but also all of the internal functions responsible for

originating and monitoring credit risks. The frequency and content of reporting should be formally approved by both the board of directors and senior management.

77. The frequency and scope of reporting should be set according to the nature of the recipient and the level of risk. The level of risk could depend, for example, on the ratings or the size of exposures.

78. Reporting to senior management should enable it to monitor the evolution of credit risk in the overall portfolio. The scope of information (e.g., rating classes, PD bands) to be included in the internal reporting may vary according to the nature, size, and degree of complexity of the business and the bank.

79. The minimum requirements of the IRB communiqué relating to reporting are specified in Annex-2 Paragraph 63. Good practice in satisfying these requirements could include providing the following information:

    - A description of the rated portfolios (amounts, number of obligors, PDs per grade, percentage of coverage with ratings with respect to the total portfolio, breakdown by entities, sectors, sub-portfolios, and business units);
    - The distribution of the overall portfolio according to rating grades, PD bands, and LGD grades, and a comparison with the previous year;
    - A comparison of realized default rates (and loss given default and credit Conversion Factors for banks on advanced approaches) against expectations;
    - The results of stress tests;
    - An estimate of regulatory capital requirements and economic capital; and
    - The portfolio's migration across rating grades.

80. In addition to the reporting mentioned above, the CRCU should address specific reports to senior management relating to the rating system review process. It is the responsibility of the CRCU to provide coherent reporting that is clearly related to target variables.

IV.3.2.2. Issues concerning AMA

81. Operational risk reporting should be an essential part of the internal reporting system and should support the proactive management of operational risk. The recipients of the reporting should be the board of directors, senior management, Internal Audit, the Risk Committee and/or the Internal Control Committees (where established), and, where appropriate, the internal functions responsible for the identifying, assessing, monitoring, mitigating, and controlling operational

risks. These internal functions could include, for example, business functions, central functions (such as IT, internal control, and accounting), and risk functions.

82. The frequency and content of reporting should be formally approved by both the board of directors and senior management. Senior management should ensure the ongoing appropriateness of the reporting framework.

83. The frequency, content, and format of reporting should depend on the recipient and on how the information will be used. Possible uses include strategic and financial planning, day-to-day management, operational risk management and measurement, public disclosure, etc.

84. The scope of information included in internal reporting may vary according to the nature, size, and degree of complexity of the business, as well as of the bank. As a general rule, the riskier the business, the more detailed the information to be provided. The frequency and format of the internal reporting should be consistent with the level of risk.

85. The design of the reporting framework is the responsibility of the bank. However, reporting could include:

- Estimates of regulatory and economic capital;
- New or improved management policies, procedures, and practices (e.g., changes in the business environment, business practices, and internal control factors);
- Risk reduction and risk transfer strategies (e.g., the effect of any expected loss deductions, cost-benefit analysis of insurance policies, mitigation and corrective actions on the business line/event type exposure and/or losses, cost-benefit analysis of the mitigation actions);
- Operational risk exposure (e.g., description of key operational risk events and drivers, and the distribution, trend, and migration of the operational risk exposure across business lines);
- Internal and (where relevant) external loss experience (e.g., event type loss analysis and comparison in term of trends, seasonality, geographical distribution, etc.);
- Identification and assessment of vulnerability areas (e.g., risk assessments, key risk indicators); and
- Quality improvements in operational risk management and measurement processes and systems.

IV.4. Risk Management Organization

IV.4.1. Independent Credit Risk Control Unit

IV.4.1.1. Objective and scope of the Unit

86. The main goal of the Credit Risk Control Unit (Annex-2, Paragraphs 64 to 66 of the IRB) is to ensure, on a regular basis, that the rating system and all of its components – rating assignments, parameter estimation, data collection, and oversight – are functioning as intended. The Credit Risk Control Unit should perform the following tasks, among others:

    - Design of the rating system (perform or review);
    - Ongoing review of the rating criteria and model development;
    - Verification of the accuracy of all risk rating grades;
    - Assessment of consistency across industries, portfolios, and geographical regions;
    - Assessment of model use;
    - Analysis of the reasons for overrides and exceptions;
    - Quantification process (perform or review);
    - Backtesting;
    - Analysis of actual and predicted ratings transitions; and
    - Benchmarking against third party data[3].

87. The results of the CRCU's regular reviews should be reported to senior management at least twice annually.

IV.4.1.2. Location of CRCU within the organizational structure

88. CRCU shall be established as a separate unit under risk management unit.

89. The CRCU function should always have high standing within the organization, and should be staffed by individuals possessing the requisite stature, skills, and experience.

IV.4.1.3. Independence of the CRCU from the functions responsible for originating or renewing exposures

90. Lack of independence of the CRCU and pressures from relationship managers could seriously undermine the effectiveness and soundness of the IRB system. Therefore, it is important how

3Some of the below-mentioned activities shall also be performed by the validation unit. Moreover, CRCU should review all the activities performed by the validation unit and re-perform those activities where necessary or make them performed again.

to ensure and enforce independence. A CRCU can generally be regarded as independent if the following conditions are met:

- The staff of the CRCU should not have any tasks to perform that fall within the scope of the activities that it is assigned to monitor and control.
- The CRCU should be organizationally separate from the activities it is assigned to monitor and control.
- The head of the CRCU should report directly to both the board of directors and senior management and the audit committee.
- The remuneration of the CRCU staff should not be linked to the performance of the activities that it is assigned to monitor and control.

91. A strict separation between the executive functions and the CRCU could have undesirable effects. For example, models developed by risk managers without the contribution of relationship managers could be rejected by the latter, or staff from the executive departments could be tempted to force some of the model's inputs (especially qualitative inputs) in order to 'adjust' the model's outcome to their assessments (affecting the use test). Consequently, staff from the CRCU and executive departments should cooperate actively in the development of the model. In order to ensure the desired independence after model development is complete, the exchange of information could best be through committees.

IV.4.2. Operational Risk Management Function

92. The Operational risk management function (ORMF) should ensure, on a regular basis that the bank's operational risk measurement processes and risk management systems and all of their components are functioning as intended. The ORMF should have sufficient resources and skills in operational risk management and measurement methods and knowledge of the processes of the bank.

93. ORMF should ensure that the following tasks and areas are performed or covered on an ongoing basis:

    - The processes related to the definition, documentation, and collection of the four AMA elements (internal data, external data, scenario analysis, evaluation criteria concerning activity environment and internal control system);
    - Measurement methodology;
    - Monitoring and reporting systems;
    - Verifying the fulfillment of the qualifying criteria, and, in particular, of the use test;

- Operational risk quantification and allocation processes, including the calculation of any haircuts (expected loss, dependence among business units, insurance), where sufficient data are available, back testing and benchmarking, and the methodology for the allocation keys.

94. The AMA Communiqué does not specify how and where the internal validation of the AMA measurement models should take place. As a rule, the people responsible for the internal validation of measurement systems and management processes should not be the same as the people responsible for their design. Any potential lack of objectivity should be offset by an independent review, as required by the fifth principle of paragraph 47 of these guidelines.

95. Any attempt to specify where in the organizational structure of a bank the ORMF should be located could be to some extent counterproductive because the activities of the ORMF could span multiple areas and business units or banks will choose a structure that fits their management and oversight frameworks. Banks generally have a central operational risk unit and some operational risk staff in the local entities. Where this is the case, the bank should ensure that the local operational risk staff follows the guidelines set by the central operational risk unit. There should be clear responsibilities and reporting lines. The Internal Audit should perform specific examinations in order to assess the 'real' degree of independence of the ORMF.

IV.5. Role of Internal Audit

96. The Internal Audit function reviews whether CRCU/ORMF are adequate from the point of view of IRB/AMA. It should therefore have an appropriate understanding of all the processes of the rating systems, including those processes which generate the estimates of risk parameters. As part of its review of control mechanisms, Internal Audit will evaluate the depth, scope, and quality of the CRCU's/ORMF's work. Internal Audit may also conduct tests to ensure that conclusions of this work are well founded. Internal Audit should also review the adequacy of the IT infrastructure and data maintenance. For banks using statistical models, Internal Audit should conduct tests in order to check data input processes. Examination of internal audit should include evaluations about use test.

97. Internal Audit should report at least annually to both the board of directors and senior management on the bank's compliance with the IRB/AMA requirements.

98. In order to strengthen its independence, Internal Audit should not be directly involved in model design/selection. However, Internal Audit units should be staffed by individuals possessing the requisite stature, skills, and experience to fulfill their duties within the scope of IRB/AMA.

99. Notwithstanding the need for independence, some cooperation between Internal Audit and the CRCU/ORMF can be desirable (for example in order to address potential weaknesses or biases in the "rating"/"operational risk" system). For instance, information on overrides detected by the CRCU in a specific portfolio or business unit should be passed on to Internal Audit so that it can assess whether the overrides stem from model biases (for example, because the model is unfit to produce ratings for specific businesses) or from a lack of independence of relationship managers. Nevertheless, it should be clear that the CRCU/ORMF has sole responsibility for the "rating"/"operational risk" systems' performance. The audit function should not be involved in day-to-day operations such as reviewing each individual rating assignment.

IV.6. Independence/conflict of interests in rating assignment in IRB

100. Independence in the rating assignment process depends on how a bank is organized and on how it conducts its lending activities. Although rating processes may vary by bank or portfolio, they generally involve an 'assignor' and an 'approver,' whose tasks and responsibilities could differ. (Their tasks and responsibilities may vary also by portfolio.) Some of the most common situations are:

Rating assignment made by relationship managers

101. Some banks have adopted 'judgmental approaches' for assigning ratings to counterparties. Such approaches entail some responsibilities for relationship managers, who are called upon to assess the creditworthiness of the obligors based on qualitative questionnaires or specific templates. As relationship managers are primarily responsible for marketing the bank's products and services, and their compensation is usually tied to the volume of business they generate, giving them responsibilities for assigning and approving ratings would give rise to an inherent conflict of interest. Credit quality and the ability to produce accurate risk ratings are generally not major factors in a relationship manager's compensation. Relationship managers may also become too close to the borrower to maintain their objectivity and remain unbiased.

102. For nonretail business banks should not delegate rating responsibility (assignment or review) entirely to relationship managers. Relationship managers should only play a partial role in the rating assignment process, carrying out preliminary credit assessment. Then the mentioned assessments should be verified by "independent" authorities. In this case, banks should offset

the potential lack of independence with controls to prevent the bias from affecting the rating process. Such controls should operate in practice and would include, at a minimum, a comprehensive, independent review of ratings by risk control functions (for example, offsite monitoring by the credit controllers, analysis of rating performances by the CRCU, and onsite review by Internal Audit). An additional way to enforce the independence of the rating assignment is to link the compensation of the relationship manager to risk adjusted performance measures (such as RAROC-risk-adjusted return on capital) based on the outputs of the IRB system.

Rating assignment by models whose outcome cannot be modified by the users

103. This solution is typically adopted for retail and consumer banking, where the large number of loans in small amounts make it essential to minimize the cost of rating assignment. In this case, the assessment of creditworthiness is basically made by the model itself.

104. Biases in model based rating assignments could stem only from errors or fraud in the input of relevant data. Consequently, independent vetting of input data becomes crucial. The CRCU should verify on an ongoing basis that the model remains predictive of risk, by means of specific validation sessions based, for example, on back testing or benchmarking of model outcomes.

Rating assignment by independent credit officers/rating committees

105. Some banks assign sole responsibility for assigning and approving ratings to credit officers or rating committees that report to an independent credit function. This solution is aimed at separating the people who 'own' the relationship and propose new credit applications from the people who are ultimately responsible for the rating assignment. In addition to assigning and approving ratings, credit officers regularly monitor the condition of obligors and refresh ratings as necessary.

106. In this approach, the relationship between relationship managers and credit officers, and the organizational structure of the bank, become crucial, essentially because the 'true' degree of independence of the credit officer/rating committee could be difficult to evaluate in practice, especially for the largest counterparties for which approval limits are set at the level of senior management or the board of directors. Another potential disadvantage of this structure is that credit officers may have limited access to borrower information. This could affect the discriminative and predictive power of ratings.

107. The role played by the CRCU therefore becomes crucial, especially with regard to the assessment of ratings' performance and the ongoing review of the rating system.

Rating assignment based on mixed approach

108. A mixed approach is sometimes used for exposures to Corporates or SMEs.

The following example is illustrative.

> The rating assignment is initially determined by statistical or judgmental models. If the relationship manager, who is responsible for data input, is satisfied with the model's outcome, then the final rating will be the model's rating. If, on the other hand, the relationship manager disagrees with the model's outcome, he can propose an 'override' to a senior officer – or to a rating committee, according to the size of the exposure.

For smaller clients (such as SMEs in retail portfolios), relationship managers are sometimes free to change the model's rating within certain limits (they typically can upgrade only by a few notches, while they are free to downgrade as much as they want).

109. When a mixed approach is used, the features of the models combined with the organizational structure of the bank become crucial. For example, if the rating model is not suited to a particular class of obligors or facilities, there will probably be a large number of overrides, and relationship managers may also be tempted to 'cheat' the model. Banks should therefore ensure that all relevant information is considered in the rating assignment process, and should take the necessary steps to identify potential rating errors. In addition, controls are needed to ensure accuracy of data inputs. Finally, all 'management overrides' should be duly motivated by the relationship managers and all relevant decisions (both confirmations and rejections of proposed overrides) should be stored, in order to allow the CRCU to perform back testing correctly.

IV.7. Reliance on the work of external auditors in the review process

110. The IRB and AMA communiqués contain several references to tasks that should be performed by an independent assessment unit. For example, AMA communiqué, Article 5(1d) states that "the operational risk management processes and measurement systems shall be subject to regular reviews performed by internal and/or external auditors." These reviews could be performed either by the bank's internal unit or by an external auditor. As the external auditor may also be involved in performing the bank's statutory audit, attention shall be paid to independence principle.

111. The Agency will seek to understand the scope of an external audit review, and specifically whether particular subsidiaries are excluded from the review, perhaps on grounds of materiality. The purpose of this requirement is to ensure that the results of the external audit review are not incorrectly taken to apply to the subsidiaries.

112. The management of a bank/subsidiary is responsible for, and has full, independent control over the review of the bank/subsidiary, regardless of whether that review is performed by an internal or external unit. The management of the bank should communicate directly with the assessment unit at all stages, and the assessment unit in turn should report directly to the management of the bank during the review.

113. The external auditor may perform an independent assessment of a vendor's technology only if there are no relationships (including commercial and/or marketing relationships) between any parts of the two companies that could compromise the independence of the assessment.

114. A bank using a vendor's methodology should also perform a review through its own Internal Audit and/or other internal assessment unit, to ensure a thorough understanding of the vendor's methodologies. Such a review should be considered reliable only if it is performed by a unit (internal or external) that is sufficiently familiar with all aspects of the reviewed systems and methodologies.