Unofficial translation

BOARD OF THE BANK OF LITHUANIA
RESOLUTION No 149

of 25 September 2008

ON THE REGULATIONS FOR THE ORGANISATION OF INTERNAL CONTROL AND RISK ASSESSMENT (MANAGEMENT)

Vilnius

(*Valstybės žinios* (Official Gazette) No 127-4888, 2008)

Acting in observance of Article 9 of the Law of the Republic of Lithuania on the Bank of Lithuania (*Valstybės žinios* (Official Gazette) No 99-1957, 1994; No 28-890, 2001) the Board of the Bank of Lithuania has r e s o l v e d:

1. To approve the Regulations for the Organisation of Internal Control and Risk Assessment (Management) (attached).

2. To repeal:

2.1. Resolution No 178 of the Board of the Bank of Lithuania of 6 December 2001 on General Provisions for Organising the Internal Control of the Bank (*Valstybės žinios* (Official Gazette) No 107-3894, 2001);

2.2. Resolution No 74 of the Board of the Bank of Lithuania of 24 July 2003 on General Provisions for the Management of Operational Risk in the Bank (*Valstybės žinios* (Official Gazette) No 77-3568, 2003);

2.3. Resolution No 61 of the Board of the Bank of Lithuania of 7 July 1995 on Approval of the Procedure of the Formation and Activities of the Loan Committee (*Valstybės žinios* (Official Gazette) No 62-1568, 1995).

3. This Resolution shall come in to force on 1 April 2009.

Chairman of the Board Reinoldijus Šarkinas

APPROVED by

Resolution No 149 of the Board of the Bank of Lithuania of 25 September 2008

REGULATIONS FOR THE ORGANISATION OF INTERNAL CONTROL AND RISK ASSESSMENT (MANAGEMENT)

(*Valstybės žinios* (Official Gazette) No 127-4888, 2008)
23 September 2010, No 03-177[*] (*Valstybės žinios* (Official Gazette) No 114-5871, 2010)
15 March 2011, No 03-31 (*Valstybės žinios* (Official Gazette) No 35 – 1698, 2011)

I. GENERAL PROVISIONS

1. The Regulations for the Organisation of Internal Control and Risk Assessment (Management) (hereinafter the Regulations) establish the main principles to be observed by a bank with a view to ensuring that internal control and risk assessment (management) of the bank is properly organised, efficient and guarantees safe and stable functioning of the bank.

2. The Regulations apply to banks, the Central Credit Union holding licenses issued by the Bank of Lithuania and *mutatis mutandis* to credit unions and foreign bank branches licensed by the Bank of Lithuania (hereinafter banks).

3. The Regulations *mutatis mutandis* apply to the financial group of the bank, if it is subject to the consolidated supervision requirements established by laws of the Republic of Lithuania and legal acts of the Bank of Lithuania.

4. The Regulations have been worked out in observance of documents issued by the Committee on Banking Supervision: Framework for Internal Control Systems in Banking Organisations; Sound Credit Risk Assessment and Valuation for Loans; Principles for the Management and Supervision of Interest Rate Risk; Sound Practices for Managing Liquidity in Banking Organizations; Sound Practices for the Management and Supervision of Operational Risk, and the following papers released by the Committee of European Banking Supervisors (hereinafter CEBS): Guidelines on the management of concentration risk under the supervisory review process; Second Part of CEBS' Technical Advice to the European Commission on Liquidity Risk Management, Guidelines on the liquidity buffers and survival periods, Guidelines on the implementation of the revised large exposures regime, Guidelines on the management of operational risks in market-related activities.

II. RISK MANAGEMENT AND SYSTEM OF INTERNAL CONTROL

4[1]. The Bank should have in place the efficient risk management system covering risk management strategy, policy, system of risk limits, other risk management tools and procedures, risk management internal control and internal audit.

[*] The Resolution shall come into force on 31 December 2010.

5. Internal control – is a continuous process during which the management and other personnel employees influencing the process guarantee:

5.1. efficient bank activities using bank assets and other resources and protection of the bank from potential losses;

5.2. reliable, adequate and timely financial and other information used both, inside the bank, for supervisory purposes or by other third persons;

5.3. compliance of bank activities with laws, legal acts of the Bank of Lithuania and other legislation, bank strategy and internal policy.

6. Internal control of bank activities shall be guaranteed by reliable and effective internal control system. Main elements of the internal control system of activities of the bank shall be the following:

6.1. appropriate organisational structure facilitating the segregation of duties as well as relationships of vertical and horizontal responsibility;

6.2. adequate internal communication system, management bodies' communication system facilitating timely decision-making;

6.3. adequate responsibility and competence of personnel;

6.4. appropriate double internal control of operational procedures;

6.5. adequate risk control and risk management;

6.6. adequate internal control procedures;

6.7. periodic assessment of internal control system and elimination of identified deficiencies.

7. Effective functioning of internal control elements referred to in points 6.1–6.7 above shall be required for the achievement of the main objectives of internal control.

8. Internal control of the bank shall be organised in observance of the following main requirements:

8.1. The supervisory board of the bank should guarantee the effectiveness of the system of internal control of the bank. The supervisory board of the bank should recognise and understand all material risks related with bank activities, measure the extent of risks acceptable to the bank and ensure that senior management of the bank takes all necessary measures for identification, measurement and control of risks. Senior management of the bank should assume responsibility for approving and regular review of the overall business strategies and significant policies of the bank.

8.2. Management bodies of the bank should have responsibility for implementing strategies and policies approved by the board; developing processes that identify, measure, monitor and control risks incurred by the bank; maintaining an organisational structure that clearly assigns responsibility, authority and reporting relationships; ensuring that delegated responsibilities are effectively carried out; setting appropriate internal control policies; and monitoring the adequacy and effectiveness of the internal control system.

8.3. Management bodies of the bank are responsible for promoting high ethical standards, and for establishing a culture within the organisation that emphasises the importance of internal controls. Management bodies of the bank should guarantee that bank employees have adequate qualification and reputation, sufficient experience and skills necessary for carrying out their duties. Bank employees, in their turn, need to understand their relevance and role in the internal controls process. Management bodies of the bank should guarantee that written operational procedures issued by the bank emphasise the bank employee's importance and role in the process of internal control and that respective bank staff is familiarised with such written procedures.

8.4. The communication system of the bank should be properly regulated (the bank should maintain a register of information provided to management bodies of the bank by each type of risk managed by the bank, specifying responsible individuals and communication periodicity).

8.5. An effective internal control system requires that the material risks that could adversely affect the achievement of the bank's goals are being recognised and continually assessed. This assessment should cover all risks to which the bank and the consolidated banking organisation is exposed (that is, credit risk, country and transfer risk, market risk, interest rate risk, liquidity risk, operational risk, legal risk and reputation risk). Internal controls may need to be revised to appropriately address any new or previously uncontrolled risks.

8.6. Control activities should be an integral part of the daily activities of a bank. An effective internal control system requires that an appropriate control structure is set up, with control activities defined at every business level. These should include: top level reviews; appropriate activity controls for different departments or divisions; physical controls; checking for compliance with exposure limits and follow-up on non-compliance; a system of approvals and authorisations; and system of verification and reconciliation.

8.7. An effective internal control system requires that there is appropriate segregation of duties, t. y. the conflicts of interests are avoided. Management bodies of the bank and managers of respective structural subdivisions should ensure that granting of rights to carry out financial and economic operations, their performance, recording and keeping is carried out separately. Areas of potential conflicts of interest should be identified, minimised, and subject to careful, independent monitoring. Each task assigned to the employee should be clear and logical and rights, obligations and responsibility – agreed upon and coordinated.

8.8. An effective internal control system requires that there are reliable information systems in place that cover all significant activities of the bank. These systems, including those that hold and use data in electronic form, must be secure, monitored independently and supported by adequate contingency arrangements.

8.9. An effective internal control system requires effective channels of communication to ensure that all staff fully understand and adhere to policies and procedures affecting their duties and responsibilities and that other relevant information is reaching the appropriate personnel.

8.10. The overall effectiveness of the bank's internal controls should be monitored on an ongoing basis (be part of the daily activities of bank employees) as well as periodically (internal and external audit, self-assessment or using other selected alternatives).

8.11. There should be an effective and comprehensive internal audit of the internal control system carried out by operationally independent, appropriately trained and competent staff. The internal

audit function, as part of the monitoring of the system of internal controls, should report directly to the board of directors or its audit committee, and to senior management.

8.12. Internal control deficiencies and incorrect management of risks encountered by the bank or violations should be reported immediately to bank managers by bank employees carrying out their duties.

III. ASSUMING AND MANAGING OF CREDIT RISK

9. [By Resolution of the Board of the Bank of Lithuania of 23 September 2010 item repealed with effect from].

10. The Bank should have in place the credit risk management strategy (policy). The credit risk management strategy should elaborate on all strategic elements mentioned in the General Regulations for the Internal Capital Adequacy Assessment Process approved by Resolution No 145 of the Board of the Bank of Lithuania of 23 November 2006 (*Valstybės žinios* (Official Gazette) No 143-5456, 2006).

11. Bank documents regulating credit risk management should conform to the type and complexity of crediting activities of the bank and be consistent with sound banking practices and requirements of the Bank of Lithuania.

12. All crediting products and processes should be appropriately regulated and documented in observance of risk assessment and internal control requirements.

13. Having regard to the scope of activities, a bank should adequately regulate credit risk assessment of specific activities (new entity, real property development companies (projects), etc.).

14. The understanding of crediting and credit risk management throughout the entire financial group of the bank should be uniform.

15. A bank should carry out continuous assessment of the impact of external environment on crediting activities of the bank and take appropriate actions to minimise adverse effects (revise established limits and requirements, etc.).

16. A bank should have in place an effective management information system:

16.1. A credit risk control unit should report regularly to the bank board, i.e. submit credit risk analysis reports covering at least the information about external environment, portfolio growth compared with budget, specifying risk costs, largest liabilities, distribution by economic activities, past-due status, largest problem borrowers, portfolio distribution by risk categories (risk grades and groups), changes of risk categories (risk grades and groups) during a certain period.

16.2. A loan committee and risk management committee should report to the bank board on a regular basis on the implementation of set goals in managing the credit risk. The contents of these reports should cover at least the aspects of assumed risk level, actual (planned) risk structure and risk management, other material changes as well as exemptions from established policies, areas subject to improvement and efforts to address identified deficiencies.

17. A bank should have in place a sound credit risk assessment system, which facilitates in:

17.1. assessing balance-sheet and off-balance sheet exposures (according to the definition of "exposure" provided for in the General Regulations for the Calculation of Capital Adequacy approved by Resolution No 138 of the Board of the Bank of Lithuania of 9 November 2006 (*Valstybės žinios* (Official Gazette) No 142-5442, 2006) by counterparty, also including assessment of overall exposures of related persons;

17.2. identifying with the help of quantitative and qualitative assessment criteria different risk categories (grades, risk groups), to which the borrowers and (or) exposures would be attributed:

17.2.1. a bank should have in place clear definitions of each risk category (range, risk group);

17.2.2. categories of risk (grades, risk groups) in the rating scale should be sufficient for proper differentiation of borrowers (exposures) on risk basis.

18. For the purpose of assessing credit risk of borrowers and (or) exposures and attributing them to risk categories (grades, risk groups), a bank shall use appropriate, clearly defined and documented criteria, as well as in cases when credit risk of a bank is transferred due to securitisation transactions or hedging. A bank should take into account financial standing of the borrower, its ability to repay the funds and where appropriate received security and cash flows of the object of security. Assessing corporate credit risk when in the opinion of the bank the amount of exposure is material, the bank should also assess:

18.1. situation of economic business area to which the borrower belongs and relationship between specific indicators of such area and general macroeconomic situation;

18.2. market position of the borrower (occupied market share, competitors, suppliers, customers, etc.);

18.3. ownership structure and management of the borrower (shareholders, managers, organisational structure, etc.);

18.4. accounting quality (e.g., evaluate whether auditor's opinion of several past years did not contain negative observations).

19. For the purpose of assessing credit risk of natural persons, a bank should evaluate:

19.1. ability of the borrower to discharge the exposure-related obligations;

19.2. assets of the borrower (savings products, bank accounts, etc.);

19.3. stability and reliability of the borrower (borrower's education, marital status, service record at the current workplace and (or) local information about repayment terms delayed by the borrower and whether the borrower has individual dwelling or leases it, etc.);

19.4. economic conditions and (or) other circumstances which might influence exposure repayment.

20. If a bank attributing borrowers and exposures to grades or risk groups applies statistical models, the latter should conform to the requirements for statistical models established in the General Regulations for the Calculation of Capital Adequacy.

21. Procedures of taking decisions on the grating (refusal) of exposures, in particular related with the assignment of tasks to respective employees should be clearly formalised, documented and be consistent with characteristics of the bank (bank size, organisational structure, nature of business, etc.).

22. Attribution (repeat attribution) of borrowers to risk categories (grades, risk groups) should be properly validated and documented. Where appropriate, a bank should enable third party to repeat the attribution of borrowers (exposures) to risk categories (grades, risk groups).

23. A bank should accumulate quantitative and qualitative information on the basis of which the decision to grant exposure to the borrower or refuse (or reconsider) it and attribute the borrower (or exposure) to the respective risk category (grade, risk group). Such information should be accumulated in one place (in a file, e-media, etc.).

24. Before deciding on the granting or refusal of a credit (or on reconsidering it), a bank should obtain sufficient information to be able to carry out full assessment of the risk of credit applied for. Information provided by the borrower's bank should be sufficient and enable employees who decide on granting of credits and evaluate credit risk, loan committee of the bank, internal and external auditors to make appropriate assessment of credit risk before granting of credit and throughout the entire period which remains until expiration of the credit agreement.

25. All information necessary for carrying out an appropriate analysis of the borrower's creditability should be obtained. If all necessary information is not received, a positive decision shall be assessed as being of increased risk and respective measures reducing risk should be established.

26. A bank should have in place a system for verification of reliability of data submitted by the borrower.

27. Transactions which do not conform to the crediting policies and other documents may be approved only upon validation of their need. These exposures may be granted only having established additional measures reducing risks. A bank should register such transactions and keep the board regularly informed about the extent of such transactions and their impact on the quality of credit portfolio and perform timely reviews of requirements established by the internal procedures.

28. A bank should be able to guarantee the identification of connected debtors and adequate assessment of their credit risk. To that end a bank should introduce adequate control and management procedures in its credit risk management system for identifying connected clients and monitoring changes of the group of connected clients. The process of identification of connected clients should be regularly revised and updated to ensure its efficiency. Interconnected groups of clients should be identified and looked-through in observance of the following principles:

28.1. A bank should seek that the interconnected clients' identification procedures are applied before assigning exposure to a person irrespective of the size of the exposure. As a minimum these identification procedures should apply at least to those exposures the value of which exceeds 2 percent of the bank capital and the process should be supported by documents.

28.2. The client's dependence to the group of interconnected clients should be identified when assigning the exposure for the first time or when the exposure reaches 2 percent of the bank

capital and subsequent changes should be looked-through as part of a regular review of the assigned exposure and also planning its increase.

28.3. For the purpose of identifying a group of interconnected clients all available information sources should be used, including publicly announced information about business relationships of the client or any other economic interdependence additional to data accumulated in the information systems of a bank, while automated procedures of the identification process should be used together with other methods of analysis, including expert assessment involving bank loan managers and risk management specialists.

28.4. Schemes with underlying assets should be analysed separately. A bank should determine whether the scheme or exposures of its underlying assets or both of them are connected with other bank clients (including other schemes) and therefore they should be treated as one debtor to limit the risk of large exposures. When the scheme with the exposure of underlying assets is a collective investment undertaking, a management company or persons to whom the assets in which the collective investment undertaking invests are attributed or both of them should be assessed for that purpose. When assessment covers persons to whom exposures to underlying assets of the scheme are attributed the bank should have in place procedures to monitor and assess developments of exposures to underlying assets of the scheme at least on a monthly basis. If a bank establishes the interconnection between several persons to whom exposures of underlying assets of one and the same scheme are attributed, such persons shall be treated as a group of interconnected clients to limit the risk of large exposures, however application of all procedures aimed at identifying and monitoring interconnections between bank clients to them shall be optional.

29. When credit risk of a bank is transferred as a result of securitisation transactions, the bank should have in place internal policies and procedures which are necessary in order to guarantee that in granting exposures, which will be fully or partially securitised, the bank will be guided by appropriate and clearly defined assessment criteria. A bank should have in place a clear process of granting, replacement, renewal and refinancing of exposures.

30. When risk arises from securitisation transactions, a bank which is the originator, sponsor or investor of such transaction, should follow respective procedures which guarantee that risk assessment and management will be carried out having regard to the economic content of the transaction.

31. It is recommended that a bank deciding whether to grant or refuse an exposure takes into account the profitability of transaction guaranteeing that direct and indirect cost and income projections are as detailed as possible and cover operational and financing costs, risk premium and are carried out in consideration of the borrower's risk and costs of capital compensation.

32. Once in six months a bank should perform *ex-post* assessment of profitability of credit operations.

33. In consideration of transaction scope, a bank should guarantee that at least two employees participate when taking a decision to grant (refuse) an exposure and that all information related with the borrower's creditability is also analysed by a special structural subdivision of the bank independent from its subdivisions responsible for granting and renewal of exposures.

34. In case of internal lending and lending to persons related to a bank, the latter should assess the nature of such transactions and conditions applicable to them, as defined under Articles 52–53 of the Law of the Republic of Lithuania on Banks (*Valstybės žinios* (Official Gazette) No 54-1832,

2004) and Articles 40–43 of the Law of the Republic of Lithuania on the Central Credit Union (*Valstybės žinios* (Official Gazette) No 45-1288, 2000; No 61-2181, 2004).

35. A bank should have in place an adequate policy of assessment of related groups of customers.

36. Organisation and control of the process of assessment of securities in a bank should be clearly defined and documented.

37. The process of assessment of internal reliability of credit risk assessment methods of a bank should be described in the bank's documents:

37.1. banks when taking a decision whether to grant and (or) refuse an exposure should carry out regular validation of expert, statistical or mixed methods used for assessment of the borrowers' credit risk, attribution of the borrowers or exposures to risk categories (grades, risk groups), measurement of value impairment or in other credit risk related processes, observing to the extent possible the Regulations on Validation and Its Assessment approved by Resolution No 140 of the Board of the Bank of Lithuania of 9 November 2006 (*Valstybės žinios* (Official Gazette) No 142-5444, 2006).

37.2. for the purpose of validation of statistical methods indicated in subitem 37.1, a bank should take into consideration both, actual cases of delay on payment terms and (or) default on obligations, and legal and economic environment and its crediting policy.

38. A bank should have in place individual credit risk monitoring and assessment system, which guarantees control over implementation of credit agreements, timely monitoring and assessment of financial condition and risk of the borrower, to guarantee early identification of potential problem credits, timely submission of information and necessary documents to a structural subdivision of a bank which deals with problem credits, etc.

39. The system of internal control of credit risk management (assessment) of a bank should guarantee that a bank has:

39.1. measures which enable to guarantee reliability and consistency of information used in taking a decision to grant (refuse) an exposure, attributing borrowers or exposures to risk categories (grades or risk groups), calculating value impairment, capital adequacy, etc. and observance of legal acts;

39.2. clearly defined and documented exposure review process which does not depend upon crediting function:

39.2.1. a bank should regularly review the quality of borrowers' creditability and exposures and its changes. In case of overdue repayment terms, impairment of exposure value or when in the bank's opinion borrower's risk or exposure amount is material, at least once a quarter during such reviews a bank should have to:

39.2.1.1. determine whether borrowers (exposures) remain correctly attributed to the respective internal risk category (grade, risk group);

39.2.1.2. if necessary, attribute borrowers (exposures) to another category. Risk category (grade, risk group) of the borrower (exposure), indicated (defined) in point 39.2.1 should be revised and, where appropriate, renewed each time upon receipt of new information related with a borrower (exposure), however, at least once a quarter. Risk category (grade, risk group) of other borrowers

(exposures) not indicated in point 39.2.1 (or of their representative sample) should be revised and where appropriate updated at least once a year. However, upon receipt of material information about the borrower or exposure, a bank should initiate a new process of attribution;

39.2.2. a bank should prepare and implement detailed procedures and systems necessary for monitoring the quality of its borrowers' creditability and exposures and its changes;

39.2.3. communication between the bank board, risk management and internal audit committees and (or) other respective subdivisions and employees related with processes of review of exposures, attribution of borrowers (exposures) to risk categories (grades, risk groups) and calculation of value impairment (i.e. written policies and procedures, management reports, audit programmes, minutes of meetings, etc.) should be clearly defined and documented.

39.2.4. responsibility and functions of all employees in the processes described in point 39.2.3 above should be clearly defined and documented.

IV. MANAGEMENT OF RISK IDENTIFIED IN THE TRADING BOOK

40. A bank should have in place the systems for monitoring transactions concluded on its own account, which enable at least once a day to:

40.1. register trading book transactions defined in paragraph 541 of the General Regulations for the Calculation of Capital Adequacy, and to calculate results and identify positions according to the same frequency;

40.2. measure the risk of trading book positions related both with specific and general interest rate risk as defined in Parts 2.1–2.2, Section VI, Chapter V of the General Regulations for the Calculation of Capital Adequacy and to assess the impact of positions of the bank's trading book on capital adequacy.

41. A bank should guarantee regular assessment of risk arising from material developments of the market or, where relevant, significant changes in parameters of a certain individual market segment. Validity and reliability of parameters and assumptions used for risk assessment purposes should be subject to regular reviews.

42. A bank which applies value-at-risk models for managing risks identified in the trading book, must observe quality requirements applicable to internal models as specified in Part 4, Section V, Chapter of the General Regulations for the Calculation of Capital Adequacy.

43. Trading book risk assessment results should be regularly communicated to bank management.

V. MANAGEMENT OF INTEREST RATE RISK

44. It is essential that a bank has interest rate risk measurement system which enables to:

44.1. measure current and planned exposures and flows related with all transactions (balance-sheet and off- balance-sheet items);

44.2. identify various different factors predetermining interest rate risks related with transactions performed;

44.3. periodically measure the effects of sources of interest rate risks (in particular when they are material) on the bank's performance and capital adequacy.

45. A bank should guarantee regular assessment of risks arising from material changes of market parameters.

46. It is important that a bank identifies the exact level of interest rate risks inherent in new products, transactions and new activities and ensure these are subject to adequate procedures and controls before introducing new strategies of products, hedging or risk management initiatives.

47. It is important that a bank takes into account:

47.1. re-pricing risk arising from timing differences in the maturity (for fixed rate) and repricing (for floating rate) differences of bank assets, liabilities and off-balance-sheet positions. Floating rate financial instruments expose a bank to the risk of unanticipated fluctuations of the underlying economic value of such instrument as interest rates vary, e.g., a bank that funded a long-term fixed rate loan with a short-term deposit could face a decline in future income when interest rates increase and deposit matures, while cash flows on the loan received from the borrower are fixed over its lifetime;

47.2. yield curve risk arises from changes in shape and (or) slope of the yield curve. These changes influence economic value of government bonds and interest income earned from them;

47.3. basis risk arises from futures concluded by a bank due to imperfect correlation in market prices of future and spot transactions. This gives rise to the basis risk from the moment of opening of the transaction position until its closure.

48. A bank may use the following internal limits for interest rate risk management purposes:

48.1. minimum limit for average interest rates on granted loans;

48.2. maximum limit for average interest rates on time deposits;

48.3. maximum limit for average interest rates on the client's funds;

48.4. minimum limit for spread between interest rates on assets generating income and liabilities relating with expenses;

48.5. minimum limit for net interest rate (margin);

48.6. limits for interbank loans (time deposits) to banks and other financial institutions;

48.7. limits for differences between assets and liabilities by maturity at the end of the accounting period.

49. The bank board or any other bank unit appointed by the board must ensure that the bank has in place clearly defined and documented system and procedures for establishing, monitoring and controlling such limits and other thresholds to ensure:

49.1. consistent application throughout the bank of indicators used to set the limits;

49.2. that it is clearly established whether particular limits are hard or soft, i.e. applicable only for early warning purposes;

49.3. that it is clearly defined whether the limits will be taken into account and (or) their implementation will be monitored ex-ante, e.g., before taking a positive or negative decision on a given transaction, or ex-post;

49.4. that a bank is able to monitor on a regular basis whether set limits and (or) other thresholds are sound and reliable;

49.5. that actions to be taken in case of exceeding particular limits are clearly identified and responsibilities of related employees are defined;

49.6. where appropriate, applicable limits and (or) other thresholds can be adjusted or new limits and (or) other thresholds applied;

49.7. the possibility to require regular submission of information about cases of exceeding internal risk limits of a bank.

50. A bank must have adequate management information system in place, i.e.:

50.1. If there is a possibility of material changes related with interest rate risks, information about such possible developments should be provided forthwith.

50.2. A bank board (or another bank unit appointed thereby) shall perform regular monitoring of the level and management of interest rate and regularly receive information which is sufficiently detailed and facilitates the assessment of both, interest rate risk related with key portfolios of a bank and aggregate interest rate risk of the bank at large.

50.3. A bank board (or risk management committee) should be informed about all cases of exceeding internal limits and reliability assessment results.

51. A bank should carry out regular validation of the limits and other thresholds and their establishment methods, monitoring and control systems and procedures. Methodological aspects of validation process and results of regular validation should be documented.

52. If in the opinion of the Bank of Lithuania the change of interest rate is sudden and unexpected, at the request of the Bank of Lithuania a bank should furnish the latter with the information about effects of such change on capital adequacy

VI. MANAGEMENT OF SETTLEMENT RISK

53. A bank must have adequate settlement risk assessment system in place:

53.1. A bank shall prove that assessment of settlement risk of various financial instruments is based on different stages of settlement process, i.e.:

53.1.1. unilateral payment order cancellation deadline,

53.1.2. deadline of receipt of funds related with purchased financial instruments,

53.1.3. moment of registration of final receipt of funds or of defaulted payment.

53.2. A bank must have in place the procedures which enable the monitoring of arising and expected settlement risk when a bank starts carrying out new transactions or when defaulted transactions cover several different stages of the settlement process.

VII. LIQUIDITY RISK MANAGEMENT

54. A bank board must ensure the liquidity risk management policy corresponding to the risk level of the bank, the relevance of risk for the financial system and bank activities. A bank board should assess the risk related with changes in maturities of assets and liabilities and guarantee that the respective level of funding is maintained. The strategy, policy and practice should take into account operations of the bank under normal and stressed conditions. All liquidity risk management related bank employees should be familiarised with the provisions of liquidity policy. The policy should be approved and regularly revised by a bank board. The liquidity risk management policy should specify:

54.1. level of acceptable liquidity risk assumed by a bank;

54.2. liquidity risk measurement methods (models);

54.3. applicable limits and (or) other thresholds of liquidity risks;

54.4. liquidity risk monitoring and control process;

54.5. current, short-, medium- and long-term liquidity management principles;

54.6. management of liquidity risk of different currency exposures;

54.7. use of respective financial instruments in managing liquidity risk;

54.8. description of liquidity of different types of assets;

54.9. diversification of the sources of financing by financial instruments, lenders, geographical areas, etc.;

54.10. liquidity risk management procedures in case of short- and long-term liquidity obstacles;

54.11. ways of planning current liabilities used by a bank;

54.12. procedure of determining liquidity buffer and liquidity counterbalancing capacity iquidity cushion.

55. Organisational structure of a bank must enable the bank to carry out effective management of liquidity risk, to implement the established liquidity risk management strategy, i.e. adequate separation of functions preventing the conflict of interests and effective system of internal control must be in place.

56. A bank must have adequate management information system in place:

56.1. if there is a possibility of material changes in the existing or future condition of liquidity of a bank, information about such possible developments should be provided forthwith;

56.2. a bank board (or another bank unit appointed thereby) shall perform regular monitoring of the level and management of liquidity risk and receive timely information which is sufficiently detailed and facilitates the assessment of both, liquidity risk related with key portfolios of a bank and aggregate liquidity risk of the bank at large;

56.3. when, in the opinion of the bank, there is significant concentration of liquid assets or current liabilities of a particular type or preconditions for material changes in the structure of such assets and (or) liabilities within the bank exist, the bank board or another unit appointed by the bank board must be furnished with information about such assets and (or) liabilities more frequently.

56.4. A bank board (or risk management committee) must be informed about all instances of exceeding internal limits.

57. A bank board or another unit appointed by the bank board must guarantee:

57.1. effective management of liquidity risk, consistency between liquidity risk management policy (policies) and processes and level of risk assumed by the bank with regard to existing and future activities. A bank should apply at least several limits adequately curbing the risk. A bank may apply:

57.1.1. a limit in case of mismatch between the difference of cash inflows and outflows and cumulative net cash flow of a respective period (i.e. liquidity mismatch). Net financing (liquidity) requirement can be expressed as percentage of all liabilities. This mismatch should be subject to conservative assessment having regard to potential price fluctuation and reduction in case of forced sale and to other factors.

57.1.2. ratio of liquid assets to current liabilities;

57.1.3. ratio of the difference between current liabilities and liquid funds of a bank and the difference between total assets and liquid funds of the bank;

57.1.4. limits on the difference between funds in correspondent accounts of a bank and liabilities to correspondent banks;

57.1.5. limits on minimum closing balances of correspondent accounts of a bank by currency;

57.2. that a bank has in place a clearly defined and documented system and procedures for setting, monitoring and controlling the limits and other thresholds to ensure:

57.2.1. consistent application throughout the bank of indicators used to set the limits;

57.2.2. that it is clearly established whether particular limits are hard or soft, i.e. applicable only for early warning purposes;

57.2.3. that it is clearly established whether the limits will be observed and their observance will be subject to ex-ante monitoring, e.g., before taking a decision to carry out or not to carry out a certain transaction, or to ex-post monitoring;

57.2.4. that a bank is able to monitor on a regular basis whether set limits and (or) other thresholds are sound and reliable;

57.2.5. that actions to be taken in case of exceeding particular limits are clearly identified and responsibilities of related employees are defined;

57.2.6. where appropriate, applicable limits and (or) other thresholds can be adjusted or new limits and (or) other thresholds applied;

57.2.7. the possibility to require regular submission of information about the level of concentration of risk and cases of exceeding internal risk limits of a bank;

57.3. internal methodologies of a bank cover the setting, measuring, monitoring and limiting of liquidity risk and liquidity risk mitigation measures, such as diversification of the sources of financing, etc.;

57.4. regular validation of methodologies referred to in item 57.3 is carried out. Methodological aspects of the process of validation and results of actual regular validation must be documented. The bank board must be kept regularly informed about the results of validation. A bank should regularly:

57.4.1. review used assumptions or expert valuations;

57.4.2. examine whether internal methodology (methodologies) are applied taking into account all cash inflows and outflows, including cash flows arising from off-balance-sheet items;

57.4.3. verify whether methodology (methodologies) is (are) consistent with type and scope of risk assumed by a bank;

57.4.4. perform ex-post review and back-testing of applied methodologies.

57.5. assignments, responsibility and goals are clearly distributed both to respective employees and (or) structural units of a particular bank and at the financial group level.

58. It is recommended that a bank prepares and describes in its internal documents (procedures) an adequate internal liquidity risk valuation and distribution mechanism, i.e. that liquidity risk management related costs are adequately distributed between business lines (structural subdivisions) in observance of liquidity needs according to liquidity risk management policy.

59. A bank should continuously measure and monitor net funding (liquidity) needs, e.g.:

59.1. analysing several alternative liquidity scenarios. A bank may analyse possible impact of different scenarios on liquidity and on the basis of such analysis set the limits referred to in item 57.1;

59.2. implement the limits guaranteeing diversification of current liabilities;

59.3. prepare and regularly review business continuity plans (guaranteeing survival) for handling liquidity crisis.

60. The process of financing in case of liquidity crisis must be defined clearly, if such financing is expected from parent banks.

61. A bank should have a measurement, monitoring and control system for its liquidity positions in key currencies used for its operations. In addition to assessing its aggregate foreign currency

liquidity needs and the acceptable mismatch in combination with its local currency commitments, a bank should also undertake separate analysis of its strategy for each currency individually.
62. A bank should have in place a mechanism for ensuring that there is an adequate level of disclosure of information about the bank in order to manage public perception of the organisation and its soundness.

VIII. MANAGEMENT OF CONCENTRATION RISK

63. A bank must have in place the concentration risk management policy approved and regularly revised by a bank board or other subdivisions appointed by the bank board.

64. Management of concentration risk should be based on the principle of proportionality, i.e. taking into account the extent and nature of bank activities, assumed risks and performed operations.

65. Concentration risk should be managed in consideration of economic developments and taking into account the impact of such developments (in particular in critical situations) on the level of concentration risk.

66. Management of concentration risk should be an inseparable part of the Internal Capital Adequacy Assessment Process (ICAAP) of a bank;

67. For the purpose of ensuring the management of concentration risk in a bank a bank board or a subdivision designated thereby shall:

67.1. approve the procedures for identifying, assessing and monitoring concentration risks (including its drivers) and reporting procedures;

67.2. establish clear limits of responsibility for employees involved in the concentration risk management process and guarantee adequate separation of functions in order to avoid the conflict of interests;

67.3. ensure that management covers all balance and off-balance sheet positions related with concentration risk;

67.4. ensure that regular analysis of actual characteristics of all most important positions related with concentration risk (e.g., profitability, delay of payment terms, risk of debtors) is undertaken in a bank;

67.5. identify sources of risk concentration material to a bank, i.e. those to be monitored and controlled and define their measurement techniques and concentration risk assessment methods to be applied;

67.6. approve concentration risk stress testing procedures in observance of General Regulations for Stress Testing approved by Resolution No 133 of the Board of the Bank of Lithuania of 11 October 2007 (Valstybės žinios (Official Gazette) No 109-4486, 2007) and other concentration risk management tools, e.g., transfer of position related risk to third parties (credit derivatives, collaterals, guarantees, securitisation); increase of the part of internal capital for covering concentration risk; establishment of percentage limit for the ratio of the value of a certain number of individual largest exposures of a bank to bank capital, assets, net profit or any other indicator; establishment of percentage limit for the ratio of the value of a certain number of largest exposures to connected borrowers of a bank and bank capital, net profit or any other

indicator; application of Herfindahl-Hirschmann index (HHI); Gini coefficient method; model based approaches and other tools;

67.7. ensure concentration risk management at two levels:

67.7.1. management of intra-risk concentrations. Intra-risk concentrations refer to the probability that risk concentration level inside a certain type of risk (e.g., credit risk, risk arising from the trading book) may be sufficiently high to cause undesirable losses to the bank from interactions between different risk exposures within a given risk category;

67.7.2. management of inter-risk concentrations. Inter-risk concentrations refer to the probability that risk concentration level between different risk categories (e.g., credit and liquidity risk, risk arising from the trading book and liquidity risk) may be sufficiently high to cause undesirable losses to the bank from interactions between different risk exposures;

67.8. with a view to ensuring management of intra-risk concentrations approve the methodology enabling employees of responsible subdivisions of a bank to:

67.8.1. assess credit risk concentration taking into account the credit risk concentration level with regard to a particular customer, product, industry or geographic location. For the purpose of making this assessment employees of responsible subdivisions of a bank should carry out the monitoring and testing of large exposures, including exposures to connected borrowers, and exposures in the same economic sectors, geographic regions or from the same activity or commodity, the application of credit risk mitigation techniques, and including particular risks associated with large indirect credit exposures (e.g. to a single collateral issuer);

67.8.2. assess concentration of risk arising from the trading book taking into account the level of concentration of risk arising from the trading book to identify correlations of exposures in the same currency, interest rate correlations of exposures, correlations of exposures arising from the same commodities, correlation of positions held-for-trading and exposures in the trading book, impact of correlations on the level of risk identified in accepted risk arising from the trading book and value of respective portfolios. Furthermore, if a bank uses VaR models in its activities, employees of responsible subdivisions shall monitor and assess relevant exposures and limits established thereon to avoid excessive concentration in relation to such exposures;

67.8.3. assess operational risk concentration taking into account the level of concentration of operational risk according to exposures arising from application of certain risk mitigation measures, dependence of the bank on a certain provider of IT services, insurance undertaking, the same business processes. Exposures shall also be assessed for vulnerability to fraud, technological or similar interruptions, correlation of other human factor related aspects;

67.8.4. assess liquidity risk concentration taking into account the level of concentration of liquidity risk according to the structure of assets and liabilities, types of funding, correlation of interbank market factors, liquidity requirements arising from off-balance sheet items, sources of funds, maturity mismatch of positions;

67.8.5. assess other significant types of risk taking account the level of concentration;

67.9. for the purpose of guaranteeing the management of concentration risk between different risk categories approve the methodology in observance of which employees of responsible subdivisions of a bank would be able to control the level of concentration assessing:

67.9.1. correlation between credit risk and liquidity risk considering the probability of negative impact of deteriorated financial condition of the borrower on the bank's cash flows and respectively the ability of the bank to timely meet its commitments;

67.9.2. correlation between risk in the trading book and liquidity risk considering the possibility of negative impact of fluctuations of such market variables like exchange rates, interest rate, commodity price, etc., as well as financial condition of the counterparty, factors of the risk of settlements, large exposures in the trading book on the ability of the bank to timely meet its commitments;

67.9.3. correlation between risk in the trading book and credit risk considering the possibility of negative impact of fluctuations of such market variables like exchange rates, interest rate, commodity price, etc., as well as financial condition of the counterparty, factors of the risk of settlements, large exposures in the trading book on the ability of the bank to timely meet its commitments;

67.9.4. correlation between operational risk and credit risk considering the possibility of negative impact of operational risk events related with fraud, occupational safety, damage to physical assets, interruption of business and systems, as well as application of credit risk mitigation measures (e.g., insurance) and creditability of provider of credit risk mitigation measures on performance of the bank;

67.9.5. other material correlations between different risk categories that are likely to have negative impact on the activities of the bank;

67.10. ensure that a bank will have in place a clearly defined and documented system and procedures for the establishment of limits and other restrictions, monitoring and control (hereinafter the system of limits) satisfying the following requirements:

67.10.1. the system of limits should limit the level of risk accepted by the bank and capture significant correlations of concentration risk factors;

67.10.2. the system of limits shall be approved at solo and consolidated levels covering both on- and off- balance sheet positions;

67.10.3. indicators used for establishing the limits shall also be consistently applied in other activities of the bank, e.g., these indicators shall be matched with indicators used when deciding to grant (refuse) exposure;

67.10.4. for the purpose of applying the system of limits it shall be clearly established whether the particular limits must be strictly observed (hard limits) or they will be used only as early warning instruments (soft limits);

67.10.5. for the purpose of applying the system of limits it shall be clearly established whether the limits will be taken into account and subject to ex-ante monitoring, e.g., before deciding to grant (refuse) exposure or to ex-post monitoring;

67.10.6. the system of limits shall be organised in the manner which enables the bank to make regular assessments of expediency and reliability of the established limits and (or) other thresholds;

67.10.7. the system of limits shall clearly define actions to be taken in case of exceeding the limits and responsibility of related employees;

67.10.8. the system of limits shall provide for the possibility (where appropriate) to adjust 9start applying) new limits and (or) other thresholds.

67[1]. A bank should carry out regular validation of limits, other thresholds and their determination methods, monitoring and control systems and procedures. Methodological aspects of validation and results of actual regular validations should be properly documented. Validation results should be regularly reported to the top managers of the bank.

67[2]. A bank should have in place an adequately organised management information system, i.e. bank managers should be provided with the possibility to monitor concentration risk level and make timely concentration risk management related decisions. Bank managers shall be informed in timely, reliable and sufficient manner about the structure of limits (established limits, their amounts, taking into account exposures related with concentration risk arising in the particular business lines, certain geographic regions, sectors and according to certain business entities); concentration risk level; observance and exceeding of limits; measures taken to avoid exceeding the limits or if exceeding the limits is established – measures taken to eliminate it; quantitative and qualitative concentration risk indicators at two levels described in item 657.7 of the Regulations, material factors giving rise to the concentration risk and measures taken to reduce such risk; validation of limits and other thresholds established by the bank as well as their establishment methods, monitoring and control systems and procedures.

IX. MANAGEMENT OF OPERATIONAL RISK

68. The bank board should guarantee that the bank has in place an appropriate operational risk management framework laying down the processes and measures of how the operational risk which is or may be assumed by a bank should be undertaken, assessed, monitored, controlled and mitigated. The operational risk management in a bank should be carried out in observance of the operational risk management policy approved by the bank's board and subject to regular reviews. Such policy should cover the processes and measures of undertaking, assessment, monitoring, control and mitigation of the operational risk which is or can be undertaken by a bank.

69. A bank should identify and assess the operational risk inherent in all material products, activities, processes and systems which should be incorporated in the operational risk management system, including such activities as outsourcing, introduction of a new product (service), functioning of information systems of a bank, market-related activities.

70. A bank should have in place an effective management information system which guarantees that the bank's board is kept regularly informed about the main aspects of the operational risk, as of a separate risk category. A bank should have in place clearly defined decision-making procedures based on information provided to top managers about the level and management of the operational risk.

71. The bank board must guarantee that internal control of the bank covers such operational risk management matters as identification, assessment and monitoring of the sources of operational risk, validation of selected operational risk management methods, assessment of the process of accumulation of historic data about operational risk and other matters relevant to the bank.

72. The system of internal control should assess the following main sources of the operational risk:

72.1. information systems (disruptions of computer hardware and software, telecommunication systems, etc.);

72.2. effects of the human factor:

72.2.1. illegal acts of bank employees (e.g., deliberate supply of wrong information; abuse of granted powers; theft; trade operations using internal information of a bank; unauthorised payments to employees; unauthorised use of confidential information; money laundering; provision of prohibited services, etc.);

72.2.2. illegal acts of non-bank employees (burglary, forgery, hacking, etc.);

72.2.3. work conditions (violation of safe conditions of work, etc.);

72.2.4. errors (entry of incorrect data, wrong management of mortgaged property, inadequate legal documents, etc.);

72.3. loss of real property (natural calamities, fire, terrorism, etc.).

73. A bank may also provide for more sources of operational risk.

74. A bank must accumulate historic data about operational risk and losses predetermined by them (firstly about those losses of the bank which are considered material on the basis of criteria established in the operational risk management policy approved by the bank) and guarantee the quality of such data. The data accumulated should cover at least such relevant characteristics of a loss event, its date, brief description of the event, reasons of the event and its links with other types of risk (e.g., credit and market risk), size of loss, decisions taken by the bank and preventive measures introduced by it with a view to avoiding its recurrence in future.

75. A bank board should ensure appropriate conditions for effective audit of management of the operational risk the scope and periodicity of which is consistent with the level of operational risk of the bank. The internal audit function of the bank shall not be directly responsible for the management of operational risk.

76. In observance of the operational risk management policy approved by the bank board, the bank should have in place clearly defined limits of responsibility of its employees, particular operational risk control procedures and limits for significant areas of bank activities, which should be subject to periodic reviews and adjusted where appropriate having regard to the degree of risk.

77. Banks should have in place contingency and business continuity plans to ensure their ability to operate on an ongoing basis and limit losses in the event of severe business disruption. These plans should be tested periodically to ensure their effectiveness in a critical situation. The general contingency plan should be periodically reviewed and updated in consideration of changes in business environment, market, products, and information systems.

78. A bank should have required competences in order to guarantee effective control over services supplementary to its activities and management of risks related with outsourcing of such services in observance of the Rules for the Outsourcing of Services Supplementary to Bank Activities approved by Resolution No 99 of the Board of the Bank of Lithuania of 10 June 2004 (*Valstybės žinios* (Official Gazette) No 98–3688, 2004).

79. A bank should measure the following main risk aspects related with outsourcing:

79.1. strategic risk (e.g., possibility that independent activities of the provider of services outsourced by a bank will be incompatible with strategic goals of the banks; the right of the bank to adequately control the outsourcing process, etc.);

79.2. reputation risk (e.g., poor quality of outsourced services; relationships with customers inconsistent with standards applicable by the bank, etc.);

79.3. operational risk (e.g., technology failures; insufficient financial capacity of the provider of services outsourced by a bank to adequately discharge assumed obligations; errors and cases of fraud, etc.);

79.4. legal risk (e.g., possibility that the provider of services outsourced by a bank might violate the requirements of laws and other legal acts; failure to implement adequate controls, etc.);

79.5. withdrawal strategy risk (e.g., a bank has no other outsourcing alternatives in the event of the existing service provider's failure to guarantee business continuity);

79.6. country risk (e.g., possibility of additional risk arising from differences in political and legal environment, when the service provider is established in another country; more complicated planning of business continuity, etc.);

79.7. concentration and systemic risk (e.g., one and the same provider of outsourced services to a bank also services many banks; each bank exercises insufficient control of the provider of outsourced services, etc.).

80. If a bank decides to introduce a new product or financial service, to change the existing product or their combination, the system of internal control should guarantee that:

80.1. extensive analysis of risk inherent in such product is performed, in particular when a bank is not experienced in such business activity;

80.2. adequate procedures for measuring the risk of a new product, setting of limits and control are implemented;

80.3. necessary restructuring of existing procedures are carried out and procedures for introducing a new product are developed.

81. The following must be provided upon introduction of a new product:

81.1. description of the new product;

81.2. assessment of main risk aspects pertaining to the new product;

81.3. establishment of internal control and risk management procedures;

81.4. review of the new product related processes (marketing, identification of customers, sales, product creation, settlement and payment);

81.5. legal issues;

81.6. employed information technologies, data communication and safety of information;

81.7. assessment of impact on profitability and capital adequacy;

81.8. personnel training and preparation of instructions.

82. The bank board must ensure that the bank has in place properly developed information technology (hereinafter IT) systems consistent with nature of bank activities and extent of operations.

83. For the purpose of guaranteeing uninterrupted and effective functioning of IT systems and reducing operational risk related with IT systems of the bank, the following IT system control and security measures should be assessed according to the procedure and periodicity established by the bank board:

83.1. administrative and organisational measures of internal control (IT organisational structure, policy regulating IT activities, standards, procedures, etc.);

83.2. hardware and software security tools (fire safety, physical security, means guaranteeing continuity in operation in emergency situations, etc.);

83.3. information security tools (adequate administration of internal and external access rights of users, prevention of unauthorised use of information, safe transfer of information, etc.);

83.4. guaranteeing information reliability (data input control, prevention of data change or destruction, etc.);

83.5. protection against unauthorised operations (measures preventing unauthorised payments using information system of a bank, protection against unauthorised changes of software, etc.).

84. A bank should have in place internal control over recording, transmission, processing and storing of electronic data. If the bank outsources all or part of these services, the outsourcing requirements established in paragraphs 78–79 shall apply.

85. A bank should assess the following main aspects of risk related with its IT systems:

85.1. inadequate software quality which, e.g., can interrupt operation of the whole system, cause material losses due to data loss and system delay until restoration of its normal functioning; indirect losses might be caused by implemented inadequate IT software security tools facilitating internal and external fraud, etc.;

85.2. inadequate security of IT, e.g., possibility of unauthorised access, failure to update antivirus software in timely manner, etc.;

85.3. security policy weaknesses, e.g., irresponsible keeping of passwords, inadequate administration of access rights, etc.;

85.4. IT risk of specific areas: special attention should be paid to those business areas where the use of IT systems is of particular relevance, e.g., retail banking, trade in securities and currencies;

85.5. data security problems, which are likely to cause losses in different business areas, e.g., possible reputation risk resulting from disclosure of confidential data of customers, etc.;

85.6. business partner's risk (arises from outsourced IT services) the relevance of which depends upon quantities of procured interrelated IT systems and processes.

86. A bank board shall be responsible for ensuring that the bank has in place the approved IT development strategy drafted in observance of the existing and future business needs of the bank with a view to ensuring adequate design, maintenance and development of IT systems.

87. A bank should have in place approved IT system development and quality control procedures to ensure the functioning of systems according as planned. IT systems of the bank must be properly documented to guarantee the possibility for their use and development in case of emergency, e.g., in the event of change of key employees.

88. A bank should have in place the tools minimising the risk of interruption of IT system functioning (e.g., caused by fire, water, hardware failures), including design of backup systems and limited access to the main IT system components granting such right only to duly authorised individuals.

88[1]. The bank board should develop and maintain an organisational structure, internal controls and a reporting system suitable for the identification, assessment, control and monitoring of operational risks in market-related activities in observance of the following principles:

88[1].1. The bank board should promote, particularly in the front office, a culture designed to support professional and responsible behaviour. The bank should have in place adequate staff management procedures to mitigate operational risks in trade under unusual conditions, in particular when there is a need to substitute a dealer or if staff change job positions between front, middle and back offices or IT.

88[1].2. Senior management should ensure that they, and the staff in the control and support functions, have the appropriate understanding, skill, authority and incentive to provide an effective challenge to dealers' activities.

88[1].3. Operational risk should be taken into account in setting objectives for, and in the assessment of, an individual's or business unit's performance in market-related activities. Objectives for business managers and traders or business units may be set in terms of a maximum acceptable level of operational risk and/or take into account the level of operational risk in the attribution of their variable remuneration. This could be done by considering, for example, the observed level of operational risk losses.

88[1].4. Internal controls and reporting system should provide for measures preventing the cases of external fraud or other suspicious acts in market-related activities of the bank.

88[1].5. Dealers should initiate transactions only when these are compliant with their set terms of reference considering the product type and established limits.

88[1].6. A bank should have in place properly predefined documentation requirements for trading activities to reduce legal uncertainties and to guarantee that the contracts are enforceable as far as possible.

88[1].7. As a general rule transactions should be initiated and concluded in the trading room and during trading hours of the bank. Trading outside the business premises of the bank (for instance by using mobile devices) should only be permitted within the scope of internal rules

that specify, in particular, the scope of permitted trading, the recording of trades and the list of authorised dealers.

88[1].8. All relevant positions, cash flows and calculations associated with a transaction (for example trading book positions, profits and losses and contingent cash flows) should be clearly recorded in the institution's IT systems with a documented audit trail.

88[1].9. A bank should ensure that they have an appropriate framework of controls over the relationships between dealers and their market counterparts.

88[1].10. Confirmation, settlement and reconciliation processes in the bank should be appropriately designed and properly executed.

88[1].11. A bank should ensure that their margining processes are working properly and that any changes are reconciled with the relevant positions on their books.

88[1].12. The system of internal control of a bank should guarantee that sources of operational risks in market-related activities are properly identified and monitored with the appropriate level of scrutiny, intensity and timeliness.

88[1].13. The nominal value of transactions/positions should be kept under strict control for monitoring operational and counterparty risks through the definition of pertinent limits;

88[1].14. The operational risk reporting system for market-related activities of a bank should be designed to generate appropriate warnings and should alert management when suspicious operations or material incidents are detected.

88[1].15. A bank should ensure the quality and consistency of internal reports and that they are appropriate to the needs of the recipients for which they are intended.

X. FINAL PROVISIONS

89. These Regulations shall apply commensurately to bank activities, i.e. they should be implemented in observance of the scope and nature of activities, assumed risk and operations performed by the bank.