Advisory Guidelines of the Financial Supervisory Authority

Requirements regarding the arrangement of operational risk management

These Advisory Guidelines have established by resolution no. 63 of the Management Board of the Financial Supervisory Authority dated 18 May 2005 on the basis of subsection 57 (1) of the Financial Supervisory Authority Act.

Part I
General provisions and definitions

1. Scope of application and purpose of the Advisory Guidelines

1.1. These Advisory Guidelines regulate operational risk management in the subjects of state financial supervision specified in subsection 2 (1) of the Financial Supervisory Authority Act (hereinafter referred to as the ***company***).

1.2. The instructions specified in the Advisory Guidelines shall be observed in conjunction with the requirements established in legislation.

1.3. The requirements established in the Advisory Guidelines constitute general requirements which a company shall take into account in the arrangement of operational risk management conforming to the needs and options of the organisation.

1.4. The scope of application of the Advisory Guidelines depends on the organisational structure and culture, business volume and risk level of a company, as well as on the legal complexity of the financial services and products offered by, and the characteristic features of risk management and accounting system of, the company.

1.5. The Advisory Guidelines aim at contributing to:

a) the identification and management of the operational risks inherent in the activities of a company in accordance with the scope and complexity of the business of the company and the previous experience of the company;
b) the capability of a company to adequately assess its operational risks;
c) the activities of a company that serve to prevent damage or loss.

1.6. In these Advisory Guidelines, operational risk is defined and recommendations are outlined on the basis of the standards contained in the document titled *Sound Practices for the Management and Supervision of Operational Risk* issued by the Basel Committee on Banking Supervision in February 2003.

2. Terms used in the Advisory Guidelines

2.1. *Operational risk* means the risk of loss resulting from inadequate or failed internal processes, people and systems, or from external events. The definition includes legal risk, but excludes strategic, reputation and system risks.

2.2. *Legal risk* means the risk of an entitled party not being able to exercise its rights or expect the performance of obligations because of the failure of the obligated party to perform the obligations assumed by it.

2.3. *Strategic risk* means the impact of competition, operating environment and supervision on the decisions, activities and accomplishment of business objectives of a company.

2.4. *Reputation risk* means the potential that negative publicity regarding the business of a company, whether true or not, will cause a decline in the customer base or in revenue, or increase expenses relating to legal assistance.

2.5. *System risk* means the risk of problems in the activities of a company having an impact on the operation of other companies and/or the entire financial system.

2.6. *Operational risk position* means the scale of loss events relating to the possible operational risk of a unit / business / product, service or other unambiguously determinable organisational part or activity of a company, expressed in a monetary equivalent.

2.7. *Risk profile* means an internal qualitative assessment of the scale of the operational risk inherent in the organisation, unit, business, product service or other unambiguously determinable organisational part or activity of a company.

2.8. *Internal control* comprises measures the employment of which is arranged by the Supervisory Board, Management Board and employees of an organisation and which are designed to provide reasonable assurance that, with a view to accomplishment of the organisation's objectives, the following is ensured:

a) effectiveness and efficiency of operations;
b) reliability and accuracy of financial reporting;
c) compliance with applicable laws and regulations.

2.9. *Internal control environment* comprises the organisational culture within a company which designs the control consciousness of the employees. Factors influencing the control environment include the ethical values and the internal formal and informal rules of conduct applicable in an organisation, the behaviour and management style of the Supervisory Board, Management Board and managers of structural units (assignment of rights and obligations, development of the organisation and its employees, etc.).

2.10. *Internal audit* comprises independent, objective, reassuring (evaluating) and advisory activities the aim of which is to help an organisation to

assess and improve the efficiency of risk management, control and management of the organisation pursuant to certain rules.

2.11. *Outsourcing* means the assignment of certain activities necessary for carrying out the day-to-day business of a company (e.g. development and management of information technology, cash management, administrating activities, personnel management, real estate management, transportation) to third persons.

2.12. *Business continuity management* comprises activities that are designed to improve the ability of a company to respond to business interruptions and to restore its key activities, systems and process within an agreed period of time, while maintaining the critical activities of the organisation.

Part II

Operational risk management

3. Identification of operational risk

3.1. Operational risk is a distinct risk area.

3.2. Each company shall formulate a definition of operational risk for its internal use. The definition of operational risk shall be based upon the scope and complexity of the business and previous experiences in the risk management of the company and shall clearly articulate the factors that may cause an operational risk in the company.

3.3. The content of a definition of operational risk shall commensurate with the business practices of a company (IT solutions used and complexity thereof; outsourcing, personnel policy, complexity of risk management relating to services and products offered; external insurance, etc.).

4. Arrangement of operational risk management

4.1. Operational risk management is a distinct risk management area.

4.2. Operational risk management shall constitute an integrated part of the corporate governance and the general risk management system of an organisation.

4.3. Operational risk management shall be accompanied by improved definition and positioning of the activities of a company, and transition from defensive activities to activities that involve the analysis of risks and prevention of loss events.

4.4. In the arrangement of operational risk management a company should take into account that operational risk losses are not always measurable and they may be incurred after a substantial amount of time and/or indirectly.

4.5. Operational risk management is a process that requires a uniform understanding of operational risk organisation-wide and it is based upon high

organisational culture along with the relevant risk culture and positive attitude toward internal control.

4.6. In operational risk management, the creation of unfounded "feeling of security" must be avoided, as this may entail the establishment of inappropriate objectives and unintended results (first of all as regards business continuity management).

4.7. In the application of these Advisory Guidelines, a company shall seek to find a solution that is optimal and economically reasonable for its organisation, while being in line with the scope of its business and comprising all legal and business units of the organisational structure. In the implementation of the requirements established in the Advisory Guidelines in the different units of an organisation, excessive bureaucracy shall be avoided and the assumptions of efficiency of operational risk management and the value added created thereby shall be taken as the basis.

4.8. The understanding of a company of the operational risks inherent in its business and the willingness to pay attention to operational risk management besides conventional risk management systems and means (analysis models and programs, stress tests, etc.) are of essence.

4.9. The distribution of obligations and responsibility between the Supervisory Board and Management Board of a company outlined in these Advisory Guidelines is to be interpreted as conditional upon the legal and organisational structure and management culture of a particular company. Appropriate and efficient arrangement of operational risk management is contingent on the establishment and implementation of the principles set out in the Advisory Guidelines in a company.

4.10. The activities of a company which relate to operational risk management should constitute an object of independent review and assessment.

5. Duties of the Supervisory Board of a company

5.1. The duties of the Supervisory Board include establishing the organisational, business and risk management structure which is appropriate for operational risk management, as well as general principles of supervising the activities of the company.

5.2. Where the volume and scope of the business of a company render it unreasonable to ensure the segregation of business and control structures, ways of risk mitigation by means of other measures shall be sought (e.g. additional controls, reporting, the so-called four-eye principle, etc.).

5.3. It is the duty of the Supervisory Board to ensure the creation of an internal control environment that supports efficient operational risk management involving all the units and activities of the company.

5.4. The Supervisory Board shall establish the definition of operational risk and the general principles (policy) of risk management and revise the same on a

regular basis, taking into account, *inter alia,* changes in the activities and operating environment of the company.

5.5. The Supervisory Board shall, in conjunction with the Management Board, allocate the resources that are necessary for continuous development and implementation of operational risk management (budgetary resources, motivated employees with relevant qualifications).

5.6. The Supervisory Board shall be aware and have a clear understanding of the major operational risks inherent in the organisation (IT, personnel), areas of activity and operating environment of the company. The Supervisory Board shall be provided with regular reports and overviews concerning the operational risk position of the company, the circumstances that have caused changes in that position, and operational loss events.

5.7. The Supervisory Board shall ensure the capability of the company's internal audit function (qualified and motivated employees) to assess the internal regulations and activities that relate to operational risk management. The scope of activities of the internal audit function shall be sufficient to obtain assurance about the adequacy and efficiency of operational risk management.

5.8. While the internal audit function should not be directly responsible for particular activities relating to operational risk management, an optimal and economically reasonable solution should be found in conjunction with the risk management units, which corresponds to the company's scope of activity and nature of risks.

6. Duties of the Management Board of a company

6.1. The Management Board shall design the organisational structure so as to ensure that areas of responsibility, scalar relationships and reporting procedures of structural units are clearly identified. The segregation of the lines of accountability and reporting of the organisations' business and control structures shall be ensured.

6.2. It is the duty of the Management Board to introduce routines in the organisation which are based on sound risk management practices (the segregation of functions, the so-called four-eye principle, etc.), see to it that the routines are adhered to, and ensure the operation of the internal control environment, using regular reports and engaging the internal audit, if appropriate.

6.3. The Management Board shall be responsible for the implementation of the operational risk management principles (policy) approved by the Supervisory Board within the organisation.

6.4. The operational risk management policy shall be implemented throughout the organisation and all the levels of staff should understand their responsibilities with respect to operational risk management and ensure the performance of the related obligations.

6.5. The Management Board shall be responsible for the development of sub-policies and internal regulations for management of operational risks inherent

in all products, activities, processes and systems. While the manager of each structural unit is responsible for the appropriateness and efficiency of the operational risk management principles and internal regulations within his or her purview, the Management Board shall clearly determine the authority, liability and procedure for reporting in order to maintain that accountability.

6.6. The Management Board shall ensure that the operational risk management policy and the internal regulations for implementation thereof are communicated to all employees in all structural units that are exposed to operational risk. Employees' clear understanding of the risk management-related rights and obligations arising from their positions shall be ensured.

6.7. The Management Board shall see to it that day-to-day activities relating to operational risk management are performed by qualified staff with sufficient experience and technical capabilities necessary for the work.

6.8. Employees responsible for monitoring and implementation of risk management in the organisation shall have authority independent of the structural units and activities they oversee.

6.9. Employees responsible for operational risk management shall consistently exchange information with employees responsible for credit, market and other risks.

6.10. The Management Board shall implement a remuneration policy within the organisation (wages, extra pays, benefits, etc.), which is consistent with the risk profile of the company and supports sound risk management practices and the internal control environment.

7. Operational risk policy

7.1. The aim of operational risk policy is to render the definition of the risk and ascertain the methods and means of identification, measurement, monitoring, mitigation and control of the risk.

7.2. Operational risk policy shall underlie the management of all the activities of the company that relate to operational risks. The content of that policy shall commensurate with the scope and volume of the company's business and cover all operational risks inherent in the activities of the company.

7.3. Operational risk policy shall contain references to areas relevant to operational risk management. These areas include, among others, physical security of the organisation, manageability of IT systems, data protection, business continuity, prevention of money-laundering, personnel policy, etc.

7.4. Depending on the scope and volume of the company's business and the nature of the services and products offered by it, the operational risk policy shall identify the activities the purpose or contents of which have a direct or indirect impact on the organisation's activities in operational risk management. Such activities include, e.g., the development of new products and services, the selection of external service providers, development activities (incl. IT), etc.

8. Identification and assessment of operational risks

8.1. The identification and classification of operational risks shall be based on the organisation-wide understanding of operational loss events. A clear identification of loss events enables a company to distinguish operational risk from credit and market risks and to quantitatively assess the operational risk.

8.2. A company shall identify and assess the operational risks inherent in all of its products, activities, processes and systems. A company shall also ensure that before new products, activities, processes and systems are introduced or undertaken, the operational risks inherent in them are subject to adequate assessment procedures.

8.3. Effective risk identification considers both internal factors (such as the complexity of the organisational structure, the nature of the company's activities, qualification of personnel, organisational changes and employee turnover) and external factors (such as changes in the industry and technological advances) that could adversely affect the achievement of the company's objectives.

8.4. In addition to identifying the operational risks, a company shall also assess its vulnerability to these risks. Effective risk assessment allows the company to better understand its risk profile and most effectively target risk management resources.

8.5. Examples of processes/activities used for identifying operational risks include:

a) Risk mapping: in this process, various sub-units or owners of business or auxiliary processes of an organisation map the risks inherent in their units/businesses/processes by risk type.
b) Risk assessment: in this process, various sub-units or owners of business or auxiliary processes of an organisation analyse the probability of occurrence and financial impact of a risk event (using the help of risk management staff and/or external consultants, if appropriate).
c) Key risk indicators: risk indicators are statistics and/or metrics (measurements), often financial, which can provide insight into the risk position of a company. These indicators are usually reviewed on a periodic basis (such as monthly or quarterly) in order to be aware of changes that may be indicative of risk concerns. Such indicators may include the number of failed transactions, staff turnover rates and the frequency and/or severity of errors and omissions.
d) Monitoring of thresholds/limits relating to risk indicators: exceeding these thresholds/limits alerts the management to the existence of spheres with potential inherent problems.

8.6. Data on a company's historical loss experience could provide information for assessing the company's exposure to operational risk. An effective way of collecting and making good use of this information is to establish a classification for systematically tracking and recording the frequency, severity and other relevant information on individual loss events.

8.7. It would be reasonable to use the classification developed by the Basel Committee on Banking Supervision as the basis for the classification system. The classification system may differ across companies, but it should, as a general rule, comprise the following types of loss events:

a) internal fraud;
b) external fraud;
c) employment practices and workplace safety;
d) customers, products and business practices;
e) damage to physical assets;
f) business disruption and system failures;
g) execution, delivery and process management.

8.8. The inclusion of operational loss events in individual classes in pursuance of the general nature of the operational loss events allows a company to assess the risk mitigation measures employed for reducing the probability of occurrence and impact of those events. The system of classification of loss events should enable a company to determine the types of events that might potentially result in material damage and provide direct information on the need for use, and the effectiveness and efficiency, of risk management measures.

8.9. In addition to the classification of operational risks by types of loss events, a company should also classify loss events by types of principal fields of business. The fields of business underlying such classification may differ across companies.

8.10. Information about loss events principally comprises usual, high-frequency, low-severity events and low-frequency high-severity events. It would be reasonable to establish a reporting system that allows tracking and recording both types of loss events, including external information about material loss events.

8.11. High-severity events in a company are generally accompanied by an improvement of the control system of the relevant sphere or activity (or the spheres or activities corresponding to the same criteria in the whole of the company), which should substantially reduce the probability of occurrence of similar loss events in the future. In order to achieve a control environment that contributes to the prevention of loss events, it is important to take notice of high-severity loss events that have occurred in organisations similar to the company in question, and of the conditions and circumstances of occurrence of these loss events. This contributes to assessment of the probability of occurrence of similar loss events and testing the operation of the organisation’s control environment and to material reduction of the probability of occurrence and/or financial impact of the loss events.

9. Operational risk monitoring

9.1. An effective monitoring process is essential for ensuring adequate operational risk management. Regular monitoring of activities offers the advantage of quickly detecting and correcting deficiencies in the policies, processes and procedures for managing operational risk, and preventing losses.

9.2. In addition to monitoring operational loss events, a company shall identify and monitor the indicators that provide early warning of an increased risk of future losses. Such risk indicators (key risk indicators) should be forward-looking and reflect potential sources of operational risk such as rapid growth, the introduction of new products, employee turnover, interruptions in transactions and activities, system downtime, etc. When thresholds are directly linked to these indicators, an effective monitoring process can help identify key material risks in a transparent manner and enable the company to act upon the (growing) risks appropriately.

9.3. Risk indicators may derive from the particular lines of business or comprise all of the areas of activity or units of a company. Examples of such indicators include:

a) the number of customer complaints;
b) the number of customer compensation events;
c) the number of interrupted transfers and transactions;
d) employee turnover;
e) the number of observations / precepts by supervisory authorities;
f) the number of failures, or manageability, of (IT) systems;
g) the number of internal policies and procedures in need of amendment.

9.4. Monitoring is the most efficient if the control system is an integral part of the activities of a company and if the relevant regular reporting is stipulated. In addition to the reports to be submitted to the manager of the sphere in question, the results of such monitoring should be reflected in the reports submitted to the Management Board and Supervisory Board, as well. The contents of reports drawn up by the supervisory function may also serve as input for the monitoring.

9.5. The Management Board and Supervisory Board shall receive regular reports from both business units and the internal audit unit (and the reports should be distributed to all the appropriate levels of management). The reports should contain internal financial, operational, and compliance data and fully reflect any identified problem areas and should motivate timely corrective measures.

9.6. To ensure the usefulness and reliability of these risk and audit reports, management should regularly verify the timeliness, accuracy and relevance of reporting systems and internal controls in general, using reports prepared by external sources (auditors, supervisors) to that end. Reports shall be analysed with a view to improving existing risk management performance as well as developing new risk management policies, procedures and practices.

10. Control and mitigation of operational risk

10.1. A company shall have policies, processes and procedures in place to control and mitigate material operational risks. A company shall review the appropriateness of alternative risk limitation and control strategies and should adjust its operational risk profile accordingly using appropriate strategies, in light of their overall risk tolerance and profile of the company.

10.2. Control activities shall be in place which are designed to address the operational risks that a company has identified. For the risks that can be controlled, a company should decide to which extent to use control activities and

other appropriate measures, and to which extent to accept these risks. For those risks that cannot be controlled, a company should decide whether to accept these risks, reduce the level of business activity involved, or withdraw from this activity completely.

10.3. A company shall establish and implement control activities and procedures for ensuring compliance with the established set of internal policies concerning the risk management system. Principle elements of this could include, for example:

a) top-level reviews of the company's progress toward the stated objectives;
b) a system of documented approvals and authorisations to ensure that activities are carried out at an appropriate level of management;
c) policies, processes and procedures concerning the review, treatment and resolution of non-compliance issues.

10.4. Although a system of formal, written policies and procedures is critical, control activities need to be carried out through a strong internal control function. To ensure efficiency, control activities should be an integral part of the regular activities of a company, which makes it possible to quickly respond to changing conditions and avoid unnecessary costs.

10.5. An effective internal control environment requires that there be appropriate segregation of duties and that personnel are not assigned responsibilities which may create a conflict of interest. Assigning such conflicting duties to employees or to sub-units of the organisation may enable them to cause losses or errors or carry out inappropriate actions. Therefore, potential conflicts of interest shall be identified, minimised and be subject to independent monitoring and review. The relevant data should be included in risk reports.

10.6. In addition to segregation of duties, a company shall ensure that other internal measures are in place as appropriate to control operational risk, such as close monitoring of adherence to assigned risk limits or thresholds; control of access to, and use of, assets and documents (ensuring security); ensuring that staff have appropriate expertise and training; identifying business lines or products where returns materially differ from expectations; and regular verification and reconciliation of transactions and accounts.

10.7. Operational risk can be more pronounced where a company engages in new activities or develops new products (particularly where these activities or products are not consistent with the company’s core business strategies) or has entered unfamiliar markets. Owing to business objectives and customary preference thereof, there is a risk that a company cannot ensure that its risk management infrastructure keeps pace with the growth in the business activity. Therefore, it is crucial in such a situation to ensure that special attention is paid to the development and operation of internal control functions.

10.8. Some significant operational risks have low probabilities but a potentially very large financial impact. While a company cannot control all risk events (e.g., natural disasters), risk mitigation tools or activities can be used to reduce the frequency and/or severity of such events. For example, insurance policies, particularly those with prompt and certain pay-out features, can be used to externalise the risk of “low frequency, high severity” losses which may occur

as a result of events such as third-party claims arising from errors or omissions, employee or third-party fraud, and natural disasters, etc.

10.9. A company should view risk mitigation tools (incl. insurance policies) as complementary to, rather than a replacement for, internal operational risk control. Consideration also needs to be given to the extent to which risk mitigation tools truly reduce risk, or transfer the risk to another business area, or even create a new risk.

10.10. Investments in banking technology and information technology security are important for operational risk mitigation. Attention should be paid to the circumstance that increased automation could transform high-frequency, low-severity losses into low-frequency, high-severity losses. The latter may be associated with an interruption or extended disruption of business caused by internal or external factors. A company should establish business continuity plans that address this risk.

11. Outsourcing

11.1. A company should establish a policy for managing risks associated with outsourcing activities and determine the terms and conditions of selection of external service providers and of entry into contracts with them.

11.2. In the selection of external service providers, a company should assess, among other things, the following:

a) impacts (financial, reputation, business continuity, etc.), if the service provider fails to comply with the terms and conditions of a contract in the expected manner and volume;
b) potential loss or damage to be incurred by the company and other parties/persons, if the service provider fails to comply with the terms and conditions of a contract in the expected manner and volume;
c) the ability to comply with supervisory and regulatory requirements (taking into account possible changes in these requirements);
d) the consumption of financial resources and time in the case of a need to replace a service provider or reinstate the provision of the service in the responsibility of the company (business continuity management);
e) the need for, and the terms and conditions of, carrying out due diligence of the service provider, and ensuring business continuity management;
f) issues relating to the ownership right in physical and intellectual property (e.g. hardware and software, licences, documentation concerning systems and processes).

11.3. Outsourcing arrangements should be based on contracts containing explicit terms and conditions that ensure a clear allocation of rights, obligations and responsibilities between external service providers and the outsourcing company. The rights and obligations of the parties to such a contract should be clearly defined, understandable and applicable. The terms and conditions of the contract should, as a general rule, contain the following:

a) the exact contents of the services to be provided, and the requirements established with regard to the volume and quality of the services;

b) the right of the company to have access to essential information concerning the services to be provided (related contracts, accounting information, etc.);
c) confidentiality of information (incl. information concerning customers);
d) the procedure for resolution of dissension and disputes;
e) rights and obligations relating to suspension or termination of the contract.

11.4. The use of an external service provider shall not reduce the capability of a company to carry out its regular activities and comply with obligations to customers, third parties and supervisory authorities.

11.5. Outsourcing activities can reduce the risks of a company by transferring certain activities to persons with greater expertise and opportunities to carry out these activities and to manage the risks associated with the activities. However, the use of external service providers does not diminish the responsibility of the Supervisory Board or Management Board of a company to ensure that the outsourced services are provided in a safe manner (incl. the protection of customer data) and in compliance with applicable laws.

12. Business continuity management

12.1. For reasons that may be beyond the control of a company, circumstances can occur that result in the inability of the company to fulfil some or all of its business obligations (incl. liquidity), particularly where the company's physical (seat, staff), telecommunications, or information technology infrastructures have been damaged or made inaccessible. This can, in turn, result in significant financial losses to the company, as well as broader disruptions to the financial system through channels such as the payments system. Therefore, a company shall establish disaster recovery and business continuity plans that take into account different types of plausible scenarios to which the company may be vulnerable, commensurate with the size and complexity of the company's operations.

12.2. With a view to the implementation of the disaster recovery and business continuity plan, a company should, among other things:
a) appoint persons participating in crisis management and business resumption;
b) carry out relevant training programmes, incl. communication with the media and public at large;
c) create and supply crisis management centres;
d) enter into preliminary agreements with possible internal and external persons and external service providers;
e) create alternative options for recording and backing up electronic data;
f) introduce the plan within the organisation and carry out awareness/readiness checks;
g) prepare communication with all interested parties.

12.3. Particular attention should be paid to the ability to restore the electronic data that are necessary for business resumption. Where the copies of such data are maintained at an off-site facility, or where the operations of a company must be relocated to a new site, care should be taken that these sites are at an adequate distance from the impacted operations to minimise the risk that

both original and back-up data and both primary and back-up facilities will be unavailable simultaneously.

12.4. A company should periodically review its disaster recovery and business continuity plan to ensure that it is consistent with the company's current operations and business strategies. Moreover, such a plan should be tested periodically to ensure that the company is able to execute the plan in the actual event of a business disruption.

Part III
Final provisions

13. Entry into force of the Advisory Guidelines

These Advisory Guidelines enter into force on 1 September 2005.