THE IMPORTANCE OF MONITORING THE OPERATIONAL RISK AT THE LEVEL OF BANKING COMPANIES

Assoc. Prof. Adela SOCOL, PhD
Lect. Tamaş Attila SZORA, PhD
„1 Decembrie 1918" University of Alba Iulia

1. Introduction

This study analyses the main stages of administrating the operational banking risk – evaluating, monitoring and reducing modalities – stressing on a set of indicators proposed for monitoring the events generating operational risk. Within the procedures of reducing the operational risk this paper insists on preventing and decreasing measures of the operational banking risk.

The information on the study theme was realized by studying the national specialty literature and international one in the field, by analyzing the legislation and by consulting the available information's from the institutions level which make studies and researches on the operational banking risk such as the Bank of International Settlement and National Bank of Romania. The direct documentation tasked to assure the information and the knowledge of the practical phenomenon of operational risk management was realized at the banking societies from Romania through studying their internal regulations.

2. The stages of administrating the operational banking risk

The procedures for administrating the operational banking risk enforce the Romanian banks to develop activities, detailed in:

1. ***Valuation*** procedures, which comprise identification, notification and measurement of the banking operational risks. Identifying an event generating banking operational risk means establishing the moment (data) when the effective banking unit in the territory or the central administration of the bank takes knowledge of this event's happening for the first time, also including the existence of a real or potential compensation demand appeared in the bank. In this way, the banking society must take into consideration at least the following *types of events generating the operational risk*: the internal fraud; the external fraud; conditions for hiring the personnel and the safety of working place; deficient practices regarding the customers, products and activities; endangering the tangible assets; interrupting the activity and defective functioning of systems; execution, delivery and management of processes.

The notification of the operational banking risk events represents the report of the event to an internal banking structure which functions in the Central administration of the banks. This type of structure centralizes the operational events for all their banking territorial unities.

Quantifying the operational banking risk means the determination of the capital necessary for covering this risk, using one of the three means of quantification mentioned by the Basel II Agreement, assumed by the Capital Requirements Directive CRD and by the national legislation – the National Romanian Bank's regulations regarding the operational risk: *the Basic Indicator Approach, the Standardized Approach*

and Advanced Measurement Approaches. Banks may choose one of the three mentioned methods.

2. ***Monitoring*** procedures, which imply registering and following the evolution of identified operational risk events. The organizational structures in each bank having responsibilities in managing the risks analyse the events generating banking operational risk and propose adequate measures, according to those events' gravity. Each banking society draws its own system of operational risk indexes, detailed on types of operational risk events.

A possible matrix of the operational risk monitoring indicators is presented in the Table no. 1 (where E1- Internal fraud; E2- External fraud; E3- Conditions for hiring the personnel and the safety of working place; E4- Deficient practices regarding the customers, products and activities; E5- Endangering the tangible assets; E6- Interrupting the activity and defective functioning of systems; E7- Execution, delivery and management of processes; E8 – Security of „electronic banking" system; E9 – Information security ; E10 – Circuit of documents into the banks and between the banking unities and on the outside of the banks; E11 – External factors). The operational risk events E8-E11 are complementary to the ones stipulated by the national legal regulations and they derive from the definition of the operational risk, generated by internal and external banking factors.

Table 1. The correlation between the monitoring indicators and the events generating operational risk at a territorial banking unit.

Monitoring indicators	**Event generating operational risk**
The number of disciplinary measures taken for fraud cases	**E1**
The number of stealing cases, unauthorized access, cases of unauthorized use of its system or in other purposes except the professional ones	**E1**
The value of losses from activities that brought prejudices to the bank through the fraud of the employees	**E1**
The number of unauthorized changes in the informational system	**E1**
The number of robbery acts, hold-ups, threatening recorded at the banking units	**E2**
The number of attempts to install malicious software on the informational system of the bank	**E2**
The number of cases when the bank received counterfeit / false documents	**E2**
The total of losses from ATM transactions resulted from: stealing, unauthorized withdrawals	**E2**
The number of employees who left the bank to go to another banking units	**E3**
The number of complaints from the clients recorded in the reporting period	**E4**
The number of complaints from the clients resolved in the reporting period	**E4**
The number of litigations recorded in the reporting period	**E4**
The number of litigations resolved in the reporting period	**E4**
The number of intimations effectuated by the employees regarding	**E4**

Monitoring indicators	**Event generating operational risk**
the informational system, recorded in the reporting period	
The value of losses of tangible assets recorded in the reporting period owed to defective practices	**E5**
The number of events that generated the losses of tangible assets recorded in the analyzed period	**E5**
The value of destructions caused by calamities or natural phenomena	**E5**
The value / number compensatory financing from insurance policies adherent to the destruction of tangible assets	**E5**
The number of disconnections of the informational and communicational systems in a certain period	**E6, E8**
The length of time in which the informational and communicational systems were disconnected	**E6, E8**
The number of defective processing of the client's data	**E7**
The number of incidents that did not respect the documents confidentiality	**E9, E10**
The number of cases when the documents were lost on the postal route	**E10**
The number of cases when the bank appealed to alternative plans concerning the security of the information	**E9**
The number of persons who administrate the documents that have a special character	**E9, E10**
The number of norms / regulations issued in the reporting period concerning the banking activity	**E11**
The number of mass-media cases in which the bank was involved, recorded in the reporting period	**E11**

After the notification of the operational risk event, the structures of the bank's headquarters, with tasks in the field of administrating the risks, analyses the effects of these events and hold forth the measures that are imposed, regarding the gravity of the respective events. With a certain established periodicity, and whenever it is imposed, the headquarters of the bank edits a report concerning the events identified at the bank, which includes proposals for measures regarding the prevention /reducing the operational risks. This report is analyzed and approved by the executives of the bank, being the support for applying the measures for prevention and reducing the operational risks.

3. In the case of ***reducing the operational risk*** procedures, the banking company sets its correction procedures of the errors generating banking operational risk in optimum time. Also, the banking companies have to take measures for increasing the security of the information processed within their territorial units and at the level of the bank's central administration. The banks have the possibility to appeal to alternative instruments of reducing the banking operational risk such as the ones provided by insurances, by which the risk is transferred to another domain.

Table 2. The correlation between the main types of operational risks, the prevention and decrease measures for the operational risk at the level of a territorial banking unit.

The type of operational risk event	***Measures for preventing/decreasing the banking operational risk***
E1- Internal fraud	*The risk: bank robbery attempt. Measures:* - Assuring the territorial units with mechanical-physical and electronic protection factors (armored doors, access code cards, cipher access, the existence of the panic button etc.); - Assuring the adequate working spaces in the territorial units and their appropriate endowment with presses and safes in order to keep safe the documents and values; - The regulations for the access system of the staff and the tierces persons in the bank; - Assuring the security with specialized staff. *The risk: reporting the operations in bad faith. Measures:* - The periodical analyze of the income and expenses accounts from their structure and content point of view; - The continuous analyze of debtors and creditors balance accounts, as well as their analytical composition; - Computerizing the reporting activity; - Checking the data transmitted by the territorial units (both the managers of the territorial units and the staff from the headquarters of the bank), after more control keys, so that the risk of bad-faith reporting the operations to be elude; - Effecting a double technical-operative checking concerning the unreeled operations, by using more applications, both in the headquarters of the bank and in the territorial units (reconciliation between the headquarters and the territorial units). *The risk: stealing the documents. Measures:* - Keeping the values and documents in safes and constantly checking their stock; - The access in the rooms where documents/instruments/values with significant stealing risk are administrated has to be assured by cipher, with card and the panic button must exist; - Restricting and controlling the access, even for the bank's staff, for the areas with significant risk (pay office, treasury, ante-treasury, informational, archive etc.); - The elaboration and implementation of the bank's internal regulations concerning the assurance of guard, security and safety in exploiting; - Installing some devices for presence detection, with auto-protection for sabotage from the staff of the bank; - Video-recording, by the television system with closed circuit, of all the entrances in the territorial units and of the areas that present a significant risk.

The type of operational risk event	*Measures for preventing/decreasing the banking operational risk*
	The risk: the employees effectuate transactions in their own name and account. Measures: - The validation of the retail operations of the client's accounts; - The periodic checking, by sounding, of the operations carried out with auto-validation by the client administrators in the client's accounts (checking the documents through which the operation was ordered, checking the signatures, framing in the established limits etc.); - The periodical checking, by sounding, of the operations carried out at distance in the client's accounts (checking the documents through which the operation was ordered, checking the signatures, framing in the established limits etc.); - Restricting the access to operations for users, by establishing access profiles at the application level; - The constant pursuance of the suspect operations (on the accounts that had no operations in a certain period of time, successive operation of low values, identical etc.); - Establishing the compulsoriness so that the main purveyors/service providers should be designated after an offer or auction selection; - Establishing a working commission that advises the effectuation of investment and repair works; - Introducing in the specific procedures, elaborated on type of activities/products, some express stipulations concerning the measures to be taken for decreasing/eliminating this type of risk; - Creating and implementing some conduct codes for the staff of the bank involved in operations that can start the manifestation of the operational risks.
E2- External fraud	*The risk: Informational fraud. Measures:* - Protecting the bank's portal against external attacks; - Realizing the access in the electronic personalized area of the bank by secured connection of http type; - Realizing the access within informational services only by access code/card/cipher; - The adequate security of the communication systems and the adherent equipments used by the bank. *The risk: Falsification of the documents/paying instruments/money. Measures:* - Applying the bank's internal procedures when it comes to knowing the clients; - Checking the client's statements by searching the databases of the Public Finances Ministry, Trade Register Office, Banking Risks Office, Credit Office, Incidents of Payments Office, and other official information sources;

The type of operational risk event	*Measures for preventing/decreasing the banking operational risk*
	- Checking the bank's own databases regarding the clients (inluding the signatures of the authorized persons), commitments, false paying documents, entities suspected of terrorism acts; - Information received through SWIFT concerning the false documents, introduced in the national or international banking circuit, must be transmitted, in the same day, to operative quarter and branch offices by post or e-mail; - In order to avoid the authentication of some false signatures, within SWIFT service, and concerning the telegraphic keys, the following measures will be taken: a. For checked documents: the confirmation of the respective signature is asked through a SWIFT or TELEX tested message. b. The endowment with equipments specific for tracking the false banknotes/counterfeit; - Using catalogues for fakes and counterfeits; - Issuing informative letters concerning the safety elements of the banknotes; - Employing qualified personnel and training them in order to improve their capacity to use the newest detecting forgery techniques *The risk: Robbery attempt. Measures:* - Assuring the territorial units with mechanical-physical and electronic protection factors (armored doors, cipher access, the existence of the panic button etc.); - Assuring proper working spaces in the territorial units, and the appropriate endowment with presses and safes in order to keep safe the documents and values; - The regulations for the access system of the staff and the tierces persons in the bank; - Assuring the security with specialized staff; - Using communication systems with police units.
E3- Conditions for hiring the personnel and the safety of working place	*The risk: The security of the space in which is carried on the pay desk activity. Measures:* - Electronic protection systems; - Pay desks endowed with bullet-proof windows or - Codified access systems in the treasury and pay desk; - The periodical training concerning the safety at the working place; - There will be made the annual insurance of the buildings and goods for: fire, floods, earthquakes, to first class insurance companies; - There will be made the annual insurance of the bank's cars against accidents; - Insurance for transporting values.
E4- Deficient practices regarding the	*The risk: Computer viruses/the defective functioning of the systems (hard/soft)/checking in documents/interrupting the activity. Measures:*

The type of operational risk event	***Measures for preventing/decreasing the banking operational risk***
customers, products and activities	*Preventing the defective functioning of the systems/avoiding the system's disconnection:* - Maintaining the optimum temperature for the system's proper functioning; - The configuration of the critical communication equipments and data servers or applications so that, when is the case, the tasks be taken over between equipments; - Assuring the communication through two different propagation environments assured by distinct providers with automatic switch in case of damages; - Doing some back-up procedures for computer and communication systems; - Realizing complex detection, monitoring and reporting systems for any type of events; - Taking over and immediately fan out the signalized incidents by a specialized structure (help desk); - Service contracts for all the functional equipments, signed with specialized firms, and the nomination of persons who follow the unreel of those contracts; - Switching the telecommunications line on the back-up system within SWIFT service, in the case of telecommunication system's malfunctioning; - Nominating IT personnel in order to survey the proper functioning of the computer systems from all the bank's critical areas. *The risk: Preventing the systems for getting infected with computer viruses. Measures:* - Signaling the Computer Department by the persons who notice the malfunctioning/viruses/disconnecting the activity; - Continuous updating with the latest anti-virus software; - Three level cleaning: external, server, working stations. *The risk: preventing the data losses/data obsolete. Measures:* - Periodically saving the information/documents on removable media; - Elaborating a general back-up and restore policy that corresponds to the rules in force, and, in the same time, covers the real necessities of the bank's computer system. - Developing procedures that meet the back-up and restore policy demands; - Realizing two safety copies for all the saved documents and their appropriate depositing (controlled access area, metallic or fire-proof safes); - Assuring backups, appropriate configured and with updated data for all the critical equipments (communication equipments, SWIFT, Reuters, cards etc.);

The type of operational risk event	***Measures for preventing/decreasing the banking operational risk***
	- Configuring the stocking environments for online data in order to assure the necessary availability (hard-disks in configuration).
E5- Endangering the tangible assets	*The risk: Selling unauthorized products, contracting errors, errors in carrying on the contracts, risks concerning the new products or changing the existing ones. Measures:* - Carrying on guidance actions of the activity within all bank's departments - Using some working procedures that regulate the product and banking services launching activity and improving the existent products; - Organizing courses and information with operative units; - A person should introduce the SWIFT messages and another person should validate them. *The risk: money laundering. Measures:* - Respecting the internal regulations concerning the prevention of money laundering inside the bank and suspect transactions, connected to financing financial criminality/terrorism. *The risk: operation's confidentiality inobservance. Measures:* - The access to information is done with authentication and authorization; - Introducing the confidentiality clauses in the contracts signed with external service providers; - Contracts signed with the providers of equipments and services are elaborated together with the specialty department and contain clauses concerning the time to answer the incidents according to the necessary demands. This action is followed by the Computer Department. *The risk: the inobservance of products and services concerning the clients. Measures:* - Respecting the evaluative deontological code; - Respecting the in force regulations and internal norms concerning the confidentiality and the work secret. *Risks concerning the exactness of cashed/paid sums from/to clients in lei/foreign currency. Measures:* - The endowment with counting and sorting the banknotes machines; - Periodically changing the pay desk personnel. *Risks concerning the inadequate sorting the cash, in lei, done by the employees. Measures:* - The endowment with counting and sorting the banknotes machines. *The risk: evaluating the deteriorated/out of date banknotes; the transport of values from the bank's headquarter to the client's headquarters; the transport of cash (lei) from/to other banks and branches of Romania's National Bank. Measures:* - Signing the contract for insuring the transported values.

The type of operational risk event	*Measures for preventing/decreasing the banking operational risk*
	The risk: Selling unauthorized products/errors in carrying on the contract/risks concerning the new products or changing the existing ones. Measures: - Carrying on guidance actions; - Constantly monitoring the funds in order to see if they were used for their specific purpose; - Using standard forms when elaborating the documentation (imposed by financing agreements), previously checked and advised by the specialty departments; when errors occur, addenda are elaborated; - Undertaking the measures for post checking the documents by specialized persons within specialty departments and within internal control and audit departments.
E6- Interrupting the activity and defective functioning of systems	*The risk: Human errors. Measures:* - Practicing the redistributing of personnel between units or within the same territorial unit; - Crating new jobs that have as purpose the validation of the operations made by front-office personnel; - Establishing informational and organizational modalities with a view to respect the approved program for the employees from the territorial units.
E7- Execution, delivery and management of processes	*Risks concerning the bank's clients. Measures:* - With a view to decrease/eliminate the risk of erroneous data registrations/incomplete documentation: checking during territorial units controls the documents that do not arrive at headquarter; organizing guidance and control actions from specialty departments. *The risk: incomplete documentation. Measures:* - Asking for information from other bank's departments/client/the part who deliver the documentation; - Checking, at the headquarters of the bank, the documentation elaborated after field displacement; - Checking during territorial units controls the documents that do not arrive at headquarter; - Organizing guidance actions; - Double checking the documents; - It is not allowed to effectuate services without complete documentation or received subsequently. *The risk: litigations/complaints/intimations. Measures:* - They are administrated according to internal procedures, by the organizational structure created at the headquarters of the bank and whose object is to resolve the intimations and complaints. *Erroneous data registrations/incomplete documentation. Measures:* - There were organized guidance and control actions for

The type of operational risk event	*Measures for preventing/decreasing the banking operational risk*
	territorial units. *Judicial risk. Measures:* - Improving and developing the organizational culture regarding the awareness of contractual risk.
E8 – Security of „electronic banking" system	*The risk: checking in/processing documents. Measures:* - Specialists from computer department must take the measures for reducing the specific risks; - Periodically saving the information on removable media; - Check in according to the regulations of National Archive; - Respecting the norms concerning the archive activity; - Constantly doing the following operations: classification, elaborating the register and keeping the documents with a view to archive them, correlated with the risk of inappropriate keeping/archive the documents; - In the job description of every employee is stipulated the clause: "respecting the internal regulations concerning the document's maintenance"; - The documents archive is made according to the bank's internal norms.
E9 – Information security	*Measures:* - Respecting the internal regulations concerning the security of the information; - Data encryption: processed data travels encrypted with specific mechanisms etc.; - Realizing a security policy that allows the secured access (user/password) to data and electronic devices used for transmitting them.
E10 – Circuit of documents into the banks and between the banking unities and on the outside of the banks	*Measures:* - Respecting the legislation and internal regulations concerning the circuit of the documents, based on their character (not secret, secret, work secret etc.); - Respecting the internal regulations concerning the record and circuit of documents within the bank: classified, not secrete, and petitions (complaints, intimations).
E11 – External factors	*Measures:* - Analyzing some operational risk events that happened in other banking systems, with a similar developing degree; - Constantly monitoring the legislation, economic conditions etc. that can influence the banking activity.

In the field of administrating the banking operational risk, at the active banking companies from Romania, there can be identified two main preoccupations:

- On one hand, *developing an efficient frame for the operational banking risk management processes*: identification, evaluation, notification, analyze and monitor procedures of the events generating banking operational risk, on internal banking plan, in order to properly correct the errors and introduce some adequate techniques for

processing and assuring the safety of the information or by transferring the risk towards other activity domains (such as certain insurances against some events generating operational risks);

- On the other hand, *creating and feeding a bank's internal database, regarding the operational risk events* identified in the bank, on the basis of a set of rules and identifying principles, quantification and monitoring the operational risk the bank is exposed to.

Any active bank from Romania adopts a certain strategy regarding the *Operational Risk Management*. Its objective is "realizing" the operational risk and the responsibilities in managing it at the entire bank's level, with a view to maintain this risk in adequate parameters in order to assure the progress of the bank's activity in proper conditions. The process of managing the operational risk is a cyclic one, implying the repetition of the same steps as in administrating the operational risk. It shows the importance of identifying the type of monitored losses, of the persons responsible for reporting the losses, of the criteria and the methods to validate the registrations. After the validation and assurance about the information's consistency process, these must be stocked in a database concerning the losses from operational risk – "Loss Database", which will be the basis for further evaluations of this type of risk. The database will comprise information concerning the registered losses, but also concerning their recovery, such as recovered sums, the moment when the recovery took place, the sources of recovery etc.

We remark the obligation of the banking societies to calculate the capital requirements for covering the operational risk, according to national regulations, adapted after the Basel II Agreement. Since 1st January 2008, as concerns the operational banking risk, it is worth mentioning that banks, Romanian legal entities, *regarding the operational risk*, 22 banks, Romanian legal entities, opted for the Basic Approach, 9 banks for the Standardized Approach and one bank for the Advanced Measurement Approach.

For applying the advanced evaluation approach in quantifying the operational risk, a credit institution must have *the capacity of splitting the internal historical data regarding the operational risk on some activity lines and loss events' categories* and can send these data to the Romanian National Bank, on its request. The activity lines are settled by the Romanian National Bank's regulations regarding the operational risk and they are according to the Basel II Agreement: *financing the commercial companies, transactions and sells, retail brokerage, commercial banking activity, retail banking activity, payments, agent services and assets' management.*

Regarding the operational banking risk events, they are also established by the Romanian National Bank's regulations and they are adapted after the Basel II Agreement: *internal fraud, external fraud, employment practices and working place safety, clients, products and business practices, damages upon the corporal assets, activity breaking and inappropriate functioning of the systems, execution, delivery and processes' management.* Criteria of allocating the losses on activity lines and on events' categories must be objective and well documented. Comparatively with these mentioned categories, we develop in this study and others categories of operational risk event and the measures for preventing/decreasing the banking operational risk.

It's obvious that only one of the Romanian banks applies the Advanced Measurement Approaches in managing the operational risk. Banks are discouraged in applying this approach because the banks internal historical data regarding operational risk generating events either don't exist or are insufficient. The quality of the statistical data for supplying the internal models may be insufficient. And the external potentially operational risk generating events must be adequately estimated,

and for this a bank needs adequate risk parameters. It is very difficult for a bank to estimate the probability and the impact of the banking operational risk generating events. The probability and impact of the risk events measuring scales (regarding the financial outcomes, strategic objectives, and the bank's reputation) are, in essence, subjective. Then these measuring scales must be correlated efficiently with operational risk events control procedures. In order to apply the Advanced Measurement Approaches a bank has to invest huge amounts for the support software applications, the training of the personnel and for the alternative instruments for managing the banking operational risk (insurance). The Advanced Measurement Approaches involve approvals for a bank from the National Bank of Romania based on complex studies and researches.

All of these aspects have discouraged the banks –Romanian legal persons – to apply the Advanced Measurement Approaches AMA. Also, the active banking institutions from Romania are not tempted to adopt in the near future internal methods for quantifying the operational risk, because the solvency is superior to the minimum level regulated at present in Romania (8%), therefore there isn't any stimulus for saving own funds by using more advanced methodologies. In the case of the banking institutions that are a part of multinational groups, the Romanian banking market may be considered too small at the group's level in order to justify the costs of implementing the Basel II advanced approaches, banks being oriented at the present towards the increase of the market rate.

REFERENCES

Flores F., Bonson-Ponte E., Escobar-Rodriguez E.	*"Operational risk information system: a challenge for the banking system",* Journal of Financial Regulation and Compliance, vol. 14, Issue 4, page 383-401, 2006;
Jobst A.A.	*"It's all in the data – consistent operational risk measurement and regulation",* Journal of Financial Regulation and Compliance, vol. 15, Issue 4, page 423-449, 2007;
Oprițescu M. – coord.	*Managementul riscurilor şi performanțelor bancare*, Editura Universitaria, Craiova, 2006;
*****	Banca Națională a României, *"Raport asupra stabilității financiare 2007"*, http://www.bnr.ro/publicații/Raport_asupra_stabilității_financiare, 2008;
*****	Basel Committee on Banking Supervision (2002) "The 2002 Loss Data Collection Exercise for Operational Risk: Summary of the Data Collected", March 2003, BIS, Basel, Switzerland, http://www.bis.org/bcbs/qis/ldce2002.pdf;
*****	Basel Committee on Banking Supervision (2002) "Sound Practices for the Management and Supervision of Operational Risk", July 2002, BIS, Basel, Switzerland, http:// www.bis.org/publ/bcbs91.htm;
*****	Basel Committee on Banking Supervision (2006) "Observed range of practice in key elements of Advanced Measurement Approaches (AMA)", October 2006, BIS, Basel, Switzerland, http://www.bis.org/publ/bcbs131.htm;
*****	Basel Committee on Banking Supervision (2006) "Basel II: International Convergence of Capital Measurement and Capital Standards: A Revised Framework", June 2006, BIS, Basel, Switzerland, http:// www.bis.org/publ/bcbs128.htm;
*****	Norma Băncii Naționale a României nr. 17/2003 privind organizarea şi controlul intern al activității instituțiilor de credit şi administrarea riscurilor semnificative, precum şi organizarea şi desfăşurarea

	activităţii de audit intern a instituţiilor de credit, publicată în Monitorul Oficial al României nr. 47/2004;
*****	Regulamentul Băncii Naţionale a României şi a Comisiei Naţionale a Valorilor Mobiliare nr. 24/29/2006 privind determinarea cerinţelor minime de capital pentru instituţiile de credit şi firmele de investiţii pentru riscul operaţional, publicat în Monitorul Oficial al României nr. 1035bis/2006;
*****	Regulamentul Băncii Naţionale a României şi a Comisiei Naţionale a Valorilor Mobiliare nr. 13/18/2006 privind determinarea cerinţelor minime de capital pentru instituţiile de credit şi firmele de investiţii, publicat în Monitorul Oficial al României nr. 1033/2006;
*****	Regulamentul Băncii Naţionale a României nr. 5/2008 privind aprobarea utilizării standard sau a utilizării standard alternative pentru riscul operaţional, publicat în Monitorul Oficial al României nr. 173/2008.