MAGYAR NEMZETI BANK

LÁSZLÓ BAKI–DR. PÉTER RAJCZY–
MÁRTA TEMESVÁRI

Assessing and Managing Operational Risks at the Magyar Nemzeti Bank

MNB Occasional Papers 32.
2004

László Baki–Dr. Péter Rajczy–
Márta Temesvári

Assessing and Managing Operational Risks at the Magyar Nemzeti Bank

The views expressed are those of the authors and
do not necessarily reflect those of the Magyar Nemzeti Bank.

Assessing and Managing Operational Risks at
the Magyar Nemzeti Bank

Authors: László Baki, Dr Péter Rajczy, Márta Temesvári

(MNB Internal Audit Department, Operational Risk Management Group)

October 2004

Published by the Magyar Nemzeti Bank

Publisher in charge: Missura Gábor

1850 Budapest, Szabadság tér 8–9.

www.mnb.hu

ISSN 1585-5678 (online)

Contents

INTRODUCTION

Efficient management of institutional risks requires a comprehensive approach and streamlined technologies of assessment and management, exercised within adequate institutional structures. The goal of the Bank for International Settlements (BIS) is to develop these technologies at an international level through its recommendations in "International Convergence of Capital Measurement and Capital Standards" (commonly known as Basel II), which aims to promote the transparent and prudent operation of financial institutions.

The new system of recommendations to replace Basel I pays special attention to operational risks with regard to certain loss events that have attracted great attention (Barings Bank, Enron, etc.). The methodology recommended for measuring operational risks is fundamentally new, the details not yet refined, and it serves as a basis for debate.
Despite this, financial institutions increasingly deal with this issue on the basis of the First Pillar on minimum capital requirements. Not only large banks with international networks, primarily targeted by Basel II, work out methods to assess their operational risks, so do central banks, for which those requirements do not apply.

This is why Magyar Nemzeti Bank, The Central Bank of Hungary (MNB) began the overview and assessment of its operational risks, thereby providing a new ground for operational risk management.
During the process of the bank-wide operational risk assessment and the comprehensive review of one of the most essential risk management tools, business continuity planning (BCP), the organisation might possibly consider the related tasks as involving excessive work.

The present study gives a description of the operational risk assessment system worked out in the MNB, and of its interrelations with the management of these risks. We would like to show that this has always been an integral part of the general activities of the bank – but now we use a different approach. There is a systemic approach in the background and the methodology is adjusted accordingly.

1. What is considered a risk?

Generally and in a positive interpretation, risk is the chance of gain, while in a negative interpretation it is the danger of loss of value.

The types of risks are introduced in the pie chart, as published on the NetRisk website. This also shows the sources of risks.

Sources: NetRisk

As seen above, so-called operational risk is mentioned side by side with the financial and business risks. Due to the nature of operational risk, it only involves the danger of loss.

Considering the above and the recommendations of Basel II, we use the following definition for operational risk:

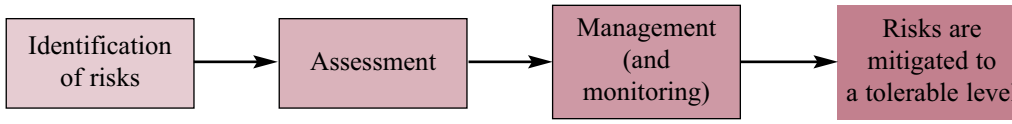
*Operational risk is defined as the risk of loss resulting from intentional or negligent behaviour of **people**, from inadequate internal **processes**, from damages or shortages of essential resources or **systems**, and from smaller or greater **external events** causing physical damages (including legal risk, but excluding strategic and reputational risk).*

We do not regard legal risk as a separate category, while we interpret the reputation of an institution as a value exposed to risks (an explanation follows later).

2. Why is risk assessed and managed?

Irrespective of whether a company is profit-orientated or not, cost-efficient management is a must. Besides being able to finance potential losses, the aim should be to mitigate them – to such an extent that they shrink to an acceptable level through proportionate efforts and maintaining the security requirements. However, it is not possible to eliminate them fully.

Risks, that is, the threats of damages, may be mitigated by risk management. In order for us to know which risks and to what extent they can be mitigated, we have to identify them and assess their level.



3. Identification and assessment of risks

3.1. WHAT IS MEASURED WHEN ASSESSING RISKS?

When assessing risks we determine the level of the threat of damages – that is, the level of risk exposure – at an institutional level, by identifying the potential loss events and estimating their possible impact.

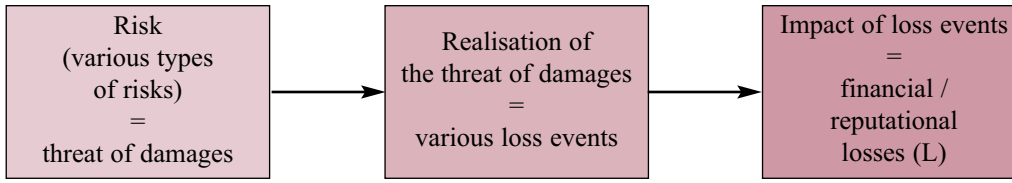
Our **values exposed to risk** i.e. the exposure indicators (EI) are the assets involved in the working processes and our credit (reputation).

Risks are realised in potential **loss events.**
These are events not considered as part of the usual working processes, due to which our values exposed to risk may suffer damages. (They may be grouped according to their character, e.g. according to Basel II the operational loss events may be grouped into seven main loss event types. See Appendix, Table 2)

The **effect** of already occurred loss events is the physical and/or moral (reputational) losses to the values exposed to risk:
- **financial losses** are the losses suffered by the bank with regard to the values exposed to risk during the working processes or the expenses not necessarily required for everyday operations (loss types include: write-downs, legal liabilities, penalties, loss of recourse, restitution, loss of or damage to assets)
The values exposed to risk here are the values used during the working processes.
The extent of these damages may be measured in money.
- **reputational losses** are the destructive effects of negative external judgement, i.e. of losing faith in the reliability of the central bank whose task is to guarantee the stability of the financial system. The loss corresponds to the damage that affects the outside world caused by the operations of the bank, and as a consequence the unfavourable picture about its operations
The value exposed to risk here is the reputation or goodwill of the central bank.
The extent of these damages may be rated, but cannot really be measured in money.

> Consequently, we do not speak of reputational risk, but conceive reputation as a value exposed to risk, to which losses of various extent may occur as an impact of various loss events.

Several operational loss events may involve a breach of law. The loss event is not the breach of law itself but, for instance, a procedural error, which also characteristically involves a breach of law. (This refers to the enactment process as well.)
Consequently, we do not speak of a separate legal risk; the financial and/or reputational losses caused by breach of law appear as an impact of the given loss event.



Risk values (the level of risk exposure) express the threat of damages and this is measured in order to establish risk management.

Probable level of impact of potential loss events
=
estimated risk value (K)

3.2. THE FRAMEWORK FOR MEASURING THE RISK EXPOSURE

Level of risk exposure is assessed within the framework of the risk matrix. The risk matrix, as a risk map, shows the location and level of the estimated risk values.

Risks are involved in the working processes. In the various working processes different types of loss events may occur, while at the same time certain types of loss events may cause damages to the exposed values of any or several working processes.
In order to assess risk values in a comprehensive way and to assure that the data do not overlap, we estimate the impact of each potential loss event in each working process and display the risk values on a table called **risk matrix**. Aggregated values can be obtained for any working process or for any loss event.

The risk map is a risk matrix displaying the estimated risk values on a table of working processes versus loss events.
The structure of the risk matrix of an institution is shown in Table 1 of the Appendix; its operational risk part highlighted with a different background colour.
The detailed operational risk matrix has been worked out adapting the Basel II recommendations.[1]

We have jointly adopted the Basel II specification of operational loss event types and the

[1] BIS, Basel Committee on Banking Supervision: Working Paper on the Regulatory Treatment of Operational Risk, September 2001.

content of the pie chart on risk types. The detailed list of loss events taken into consideration is set down in Table 2 of the Appendix.
The set of standardised working processes of the MNB is shown in Table 3 of the Appendix.

The **operational risk matrix** contains the estimated risk values as the financial impact of the potential operational loss events identified in the working processes, based on assessed and estimated data.

It is also justified to take into consideration **business** (strategic and management) **risks** across the various procedures of working processes because it is considered to be of substantial level. The identification and quantification of business risk like loss events (e.g. errors in professional decision-making) seems to be difficult. Their financial impact on the external institutions and on the clients, however, may correspond to the level of reputational damage of MNB. This is why we plan to propose prioritisation of working processes based on the reputational impact of business risk like loss events. Prioritisation should be made by the top management.

From the point of view of our study, we have not considered the separately measured and managed **financial risks** (credit, market and liquidity risks) but they may also fit into the system. Through this extension that would require top management decision, an institutional risk map may result covering each working process and all the three main types of risks, that is, the total risk exposure.

The risk map extended for business risks shows quantified operational risk exposure and (we would hope) it also shows the priority of working processes according to business risk exposure. Together, these may provide information on the risk exposure of working processes excluding financial risks.

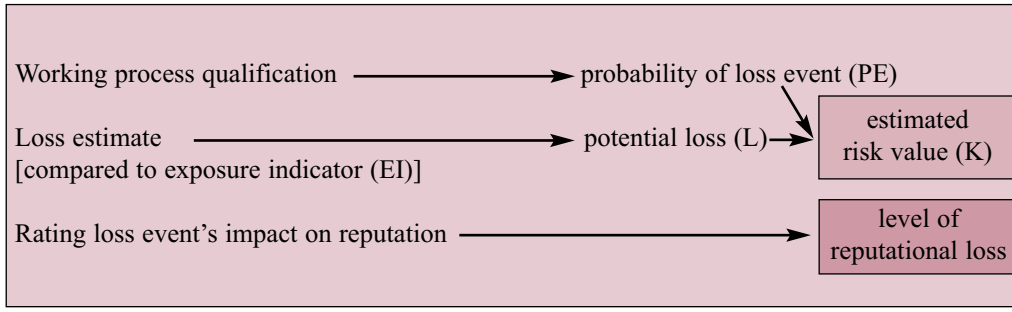
The result is subject to change over time. By updating the risk matrix the changes in working processes may be monitored. Regularly repeated surveys, as well as the estimation of the values exposed to risk in the working processes and the risk values reflecting the effects of quality changes, can result in a proactive risk map. Consequently, taking changes in risk exposure into consideration, the risk management processes can also be updated.

3.3. MEASUREMENT METHODOLOGY

Operational risk values are estimated by the application of a model that uses qualifying factors to determine the probability of the occurrence of loss events on the one hand, and potential damages caused by them on the other.
In addition, the level of reputational loss for each loss event in each working process can also be assessed.
Historical loss data are also collected.

We have adopted the AMA methodology (Advanced Measurement Approach) of Basel II to assess the potential losses arising from operational loss events. Being a central bank, the aim of the chosen method is not to determine regulatory capital but to have a comprehensive overview of risk values and to foster risk awareness (by the method itself); therefore it is built on self-assessment of the business units responsible for the working processes. At the same time, we had to accept the limitations due to scarce data sources and lack of experience.

Elements of the process:



Probability of loss event (PE) is a calculated figure derived from the qualification of the working process and from internal model parameters.

Working processes are qualified by evaluating standard qualitative criteria (qualifying factors) from various points of view, which are in relation to the current situation of operational risk management tools.

Only the relevant qualifying factors for the given loss event are to be taken into consideration.

In the case of certain loss events, the probability of loss events of those working processes are assigned to the potential loss, the quality of which significantly influence the occurrence of the loss (e.g. in the case of disruptions in telecommunication the quality parameters of the working process relating to the purchase of assets and services ensuring the general working conditions were assigned to each working process).

During the evaluation process, special attention is paid to the key risk indicators (KRIs),[2] characteristic of the working process from the point of view of the given qualifying factor.

In our model the qualifying factors rating the actual quality of the process are as follows: *level of control strategies and practices (C), human factors (E), effects of changes (V), level of IT/infrastructural support (I), level of preparedness for emergencies (K)* (see Figure 1 in the Appendix).

[2] Key Risk Indicators (KRIs) are the most essential characteristics to be measured in the process, through the monitoring of which we can notice in time if the level of risks in the process has increased by a significant extent.

When rating the qualifying factors, the effect of the different risk management tools (i.e. what KRIs reflect) shall be evaluated by the business units. For *C, E* and *V* regulation and quality management, for *I* protective measures and regulations, for *K* BCP/DRP, plans for prompt intervention measures and insurances are to be evaluated. (See risk management tools at the bottom of Table 1 in the Appendix. A detailed explanation follows later.)

The qualification is made by self-assessment, with audit corrections.

Potential loss (L) is the annual financial loss (i.e. write-downs, legal liabilities, penalties, loss of recourse, restitution, loss of or damage to assets) estimated within the working processes by each loss event.

When determining potential losses, the estimated value of exposure indicators (EI) (i.e. assets: turnover, balance, physical assets, wages) involved in the working process shall serve as a limit. The annual level of potential losses is estimated on the basis of this limit by thinking over the possible scenarios of individual loss events. The value of potential loss is naturally higher than the risk value because the probability factor is not taken into account here.

In the case of certain loss event types (damages to physical assets), we uniformly took into consideration an insurance tariff in proportion to the EI, which already incorporates probability when estimating the potential losses. In other cases (employment practices and workplace safety), we estimated the loss in proportion to the EI using standard proportions fixed for all processes.

The actual values of exposure indicators (EI) serving as a reference are collected annually (general ledger accounts, interviews) in order to support determining their estimated level.

The estimation is made by self-assessment.

Estimated risk values (K) are calculated by multiplying the probability of loss events (PE) (characteristic to the process quality rating) and the potential losses (L) assessed by each loss event.

Risk values calculated with the above method are gross losses. This means that the recoveries are not considered by the estimates. They are taken into consideration in risk management (the loss database also includes this information).

Although it would be justifiable to consider more factors when determining the probability of loss events and the potential damages (e.g. central bank risk profile index, external and internal historical loss database) these factors have not been taken into consideration in this model due to the lack of information. (The institutional loss database has been built for two years, but it serves only as a limited basis for comparison with potential losses.) We kept the model parameters at their initial values and they may be modified when further experience is gained. The result provides guidance to the proportions of estimated risk values but the level of their accuracy is yet to be verified.

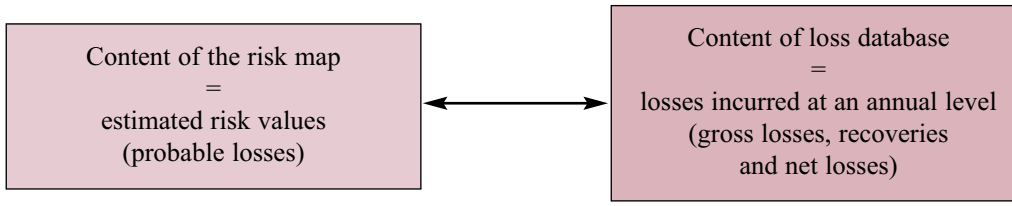
The scheme of the whole process is summarised in Figure 1 of the Appendix.

Within the working processes, **the impact of the individual loss events on reputation** shall be rated by qualification.
The aim is to localise the loss events that do not necessarily result in a financial loss but will damage the reputation of the bank due to the inconveniences they cause (e.g. waiting time, adjustment of errors). These threats shall be considered when the consolidated evaluation of the working processes is prepared and when the risk management strategy is created.
The qualification is made by self-assessment.

The form used for the assessment is shown in Figure 2 of the Appendix.

The **historical data** relating to operational risks are collected in the loss database.
The annual value of gross losses and recoveries, and the net losses calculated as their difference shall be structurally incorporated into the operational risk matrix. In this way it will facilitate comparability with the estimated figures.
The aim of data collection is manifold. To a certain extent, these data serve as a reference when assessing the risks. They support a more accurate estimation process (model) in the long run and they serve as a guideline for the daily maintenance of risk management tools.
The procedure is centralised, including data collected from the general ledger accounts (relating to the categories considered in the case of potential losses) as well as interviews.

The data of the loss database obviously can differ from the estimated risk values in the given year or their overlap is incidental.



3.4. SIGNIFICANCE OF THE SET OF STANDARDISED WORKING PROCESSES

A working process consists of well-defined steps of operational tasks and has certain objectives, inputs and outputs. It includes decision-making and its forums, organisational measures, and is – in its parts or as a whole – under management control. The framework that includes each working process, grouped hierarchically, is the set of standardised working processes.

A well-built set of standardised working processes can serve as a basis to effective operation and to efficient operational risk management.
In order to be efficient, we should assign the various institutional characteristics to the working processes in a consistent, comprehensive and not overlapping manner. Therefore the structure of the working processes has to be configured so that everyone within a bank

can interpret the processes in a uniform manner and so that it would be least affected by organisational changes and by any modification of the division of tasks and responsibilities.

The set of the standardised working processes is organised in the operational risk matrix as follows:

Institutional functions ('Functions') (i.e. Business units in Basel II terminology), various business lines ('Business lines') that fulfil functions through the activities ('Activities'). Working processes ('Working process'), centred to activities, are groups similar in their characters, aims and transactions. Working processes consist of joining or parallel task completion chains of various business units.

The set of standardised working processes in the MNB was created on the basis of the Basel II recommendations for the general division of financial institutional functions (see Table 3 of the Appendix). However, the recommendation goes down to the 'Business lines' level only.
The central banks are not special subjects of this recommendation. The working processes of several central banking activities, however, are comparable to those of commercial banks. The special central banking activities are grouped into a separate 'Central Banking' function, similarly to other special activities (see 'Others').[3] With this division, we also wanted to make our set of standardised working processes comparable with that of other financial institutions. In addition to a more detailed breakdown, we only deviated from the generally recommended system in a way whereby we separated the supporting and supply functions. (It would be desirable to compare our working process structure with other banks carrying out risk assessment and collecting loss data and exposure indicators; however, other financial institutions have not yet published such data in detail.)

Why do we consider it important to establish a set of standardised working processes and define the individual working processes?

The reason is that, if continuously updated, this provides a framework for the unified structure of certain essential institutional characteristics (e.g. external/internal regulations, process expenses, data relating to human resources, assets and various risks) in the bank as a whole, as well as their monitoring. This may contribute to providing a basis for certain planning tasks.

[3] BIS, Basel Committee on Banking Supervision: Working Paper on the Regulatory Treatment of Operational Risk, September 2001. Annex 2, p. 21

4. Management of risks

4.1. How can the risk map be utilised for risk management?

Efficient risk management means cost-efficient risk mitigation.

Mapping risks provides orientation for risk management; it shows which risks should be managed in which working process, thereby making the supervision of risk management efficiency more reliable.

The risk map containing comprehensive information for making decisions on evaluating existing processes or introducing new ones provides support in the following ways:

- The starting point of risk management is the detailed analysis of the risk matrix. That means the simultaneous evaluation of the set of the assessed and localised risk values and the reputational risk levels, assigned to working processes and individual loss events; supplemented later by the analysis of the priority list. As a result, working processes can be ranked in accordance with their risk exposure. The relevance of loss events may be ranked as well. This helps in deciding which risk is worth managing and how much should be devoted to this purpose, and whether the potential investment projects planned within this framework are proportionate to the risks. (The management of the risk should not cost more than the level of risk itself and attention should be paid to the highest localised risks.) Finally, comprehensive information will be supplied as a basis for top management decisions.

- Within the framework of creating and supervising the risk management practice, it may be decided which business unit, who shall manage the relevant risks and how, with special regard to occasional and continuous expenses. When weighing up the methods of risk management, one needs to consider that risk values alone are not indicative enough (they may come from several small or a few large damages as well). Various scenarios and effects need to be analysed in order to choose the appropriate method.

Determination and supervision of the risk management procedure:

- preliminary evaluation

  - analysis of the risk map, identification of the concentration of risks, defining the risks and working processes to be managed or to be supervised
  - evaluation of key risk/early warning indicators and loss data (analysis of loss data, errors, audit issues, measures) in the given working processes, analysing the scenarios of key loss events, impact analysis

- choosing the optimum risk management method

  - defining the steps and tools of the risk management process, cost-benefit analysis (one-off and permanent costs)
  - defining the organisational framework (regulations, setting down the method of implementation and monitoring, allocation of responsibilities).

4.2. OPERATIONAL RISK MANAGEMENT

The management of operational risks is an existing practice that is linked to the banking operations in different phases. The methods and organisational framework, however, need maintenance according to the changing situations revealed in the risk map.

The most characteristic tools used in the various operational risk management phases assigned to loss event types (the most comprised the seven loss event types of Basel II) are shown in Table 1 of the Appendix.

The characteristic tools of operational risk management in the phases of prevention, managing emergency situations and preliminary measures for damage compensation schemes are as follows:

Prevention – rules and continuous processes basically serving the purpose of fending off or quick discovery of loss events

– Internal regulations (or in its most developed form, a flow chart) containing the checkpoints built in the process take care of process risk mitigation through the establishment of control. Risk management not only means developing the checkpoints set down in regulations but also ensuring their proper operation and continuous built-in control. Regulations need to be updated in a timely manner.
Quality management is the supervision of the working process from the point of view of control and efficiency, and, if necessary, restructuring it. This can be interpreted as an internal regulation tool.
– Protective measures (technical and human protection, screening, system monitoring) also mitigate risks with the purpose of prevention. They ensure the protection of assets, persons, sensitive information, as well as the prevention of crime in the relevant working

processes or areas, through fire and foray protection, human safety and IT security, protection of sensitive data, prevention of money laundering, labour and environmental protection, as well as civil defence regulations and measures. (In addition, there might be plans of prompt intervention to be applied in certain emergency situations.)
It is important to have technically advanced, lawful and functioning systems at the ready.

Managing emergency situations – systematic business continuity planning (a BCP-system) is a set of measures to smoothly and quickly restore operation and mitigate losses in the case of the occurrence of loss events.

– BCP (Business Continuity Plan) – an action plan that serves the purpose of mitigating losses by applying alternative working processes to ensure the management of crisis situations, including working at an alternative place.
It is important to have usable and tested action plans always at one's disposal.
Prompt intervention consists of pre-defined emergency measures to be taken subject to the nature of process and risk, e.g. rescue, evacuation, fire fighting, informing the police or other authorities, stopping the working process, requesting prompt inquiry, immediate external communication. These are basically scenarios to mitigate the risk as quasi action plans, and are not part of the BCP action plans.
It is important for all involved to be aware of these measures and to be able to apply them.
– DRP (Disaster Recovery Plan) – an action plan that serves the purpose of mitigation of damages in emergency situations by securing the restoration (repair or replacement) after breakdown of essential resources. This is primarily conceived for IT resources, but DRP may be prepared for other technical resources as well. The plan is often supported by a service contract.
It is important to have usable and tested action plans and service contracts with the relevant conditions at the ready.

Preliminary measures for damage compensation schemes – conclusion of contracts guaranteeing compensation for damages in persons or assets within or outside the institution

– Property, liability and life insurance schemes mitigate potential damages to a calculable level via preliminary measures for damage compensation schemes.
It is important to have up-to-date insurance policies fitting the current situation, proportionate to the institution's risk appetite.

4.3. HIGHLIGHTED: BUSINESS CONTINUITY PLANNING (BCP)

Business continuity planning, as one of the most essential operational risk management tools, serves the purpose of managing operational breakdown periods in emergency situations as follows:
An assessment is made for each working process within the MNB (and for each stage of the given working process that is easily separable from the business continuity point of view) concerning the level of financial or reputational damages that may occur in the case of an outage caused by a shorter or longer disruption in the availability of an essential resource. (The result should naturally be in line with the values given when assessing the operational risks). In the case of breakdown of resources, necessary to those activities this assessment found critical, BCP action plans which offer alternative processes are prepared. DRP action plans are also prepared for restoring these breakdowns. In our system these are mostly IT applications or other resources, but action plans may also be prepared for human resources or location problems.
An action plan determines – in the case of necessity – the way highly important working processes can be transferred to an alternative location (backup or split site) where carrying out work and securing the conditions is possible.

Action plans are ready for use after they are certified and tested. Therefore, great emphasis should be paid to having a tested action plan for each emergency 'BCP' situation. The essentially needed prompt interventions should also be known.

A centralised system provides the documentary background for the overview and maintenance of the above at the bank level. Preparation, maintenance (updating and testing) of the BCP and DRP action plans is the duty of the business units (local BCP officers) involved. Tests requiring the cooperation of several business units may be carried out with the coordination of the affected units, in some cases requiring the participation of the Crisis Committee.

4.4. MONITORING THE QUALITY OF RISK MANAGEMENT

Monitoring the quality of risk management is part of the risk management activities of the business units, accompanied by management control. Internal Audit evaluates risk management during the audits. To give orientation for both activities, the risk map serves as a basis of information. Comprehensive risk assessment reflects the results of risk management through the change in qualification of working processes.

- The **business units monitor** the effect of their risk management measures.
The process manager should regularly update the key risk indicators (KRIs) characteristic to the process, with special regard to the risk management measures taken and the loss events occurred or almost occurred in spite of these measures and the audit issues. The process manager reviews the early warning factors that may be used for prevention and determines whether the built-in controls need to be modified at the regulatory or implementation level. He checks whether the prompt intervention measures and action plans

prepared for emergency situations are adequate and useful, i.e. whether certifying and testing took place in order.

It may be reasonable to uniformly and regularly prepare the documentation and reporting on loss events, evaluations and measures. Top management controls this and orders further measures if necessary.

– Internal Audit

Internal Audit evaluates the quality of risk management during its process audits included in its annual plan. It examines the efficiency of risk management tools and their application, including management control, and whether the risks have been mitigated to an acceptable level.

The inputs for preparing the audits are the process description (internal regulations), the operational risk map (potential loss events and their probable effects), the KRIs selected during risk assessment, the loss database information and former audit issues.

– The risk map shows what risks the business unit considered relevant. Their reality and the method of risk management, including the content of BCPs and DRPs are to be evaluated. It may be reasonable to assign the audit issues to loss event types.

– It can be checked whether KRIs have been established and monitored, whether action plans have been prepared, whether their efficiency has been analysed, and whether there is management control (whether reporting exists) and what related damages incurred.

– If the risk management plan needs investments into goods, it can be checked how well founded this is.

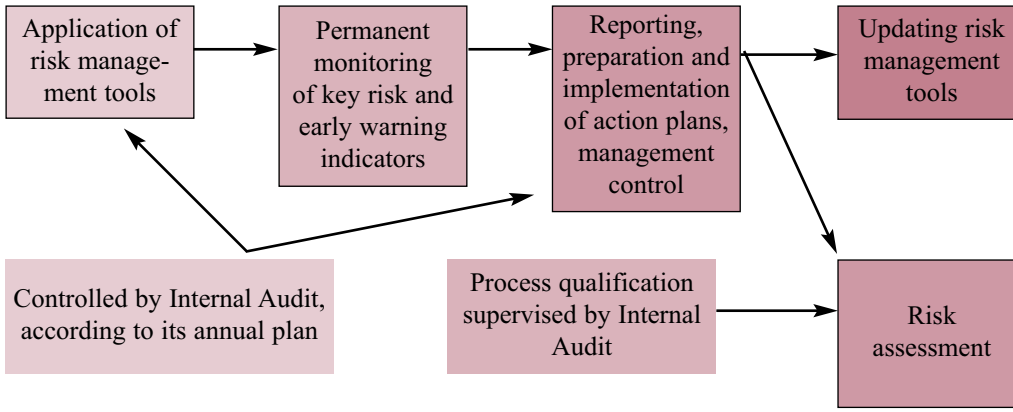
– Comprehensive risk assessment

The effects of risk management tools are measured during the annual operational risk assessment process through the evaluation and rating of process qualifying factors given by the business unit, and complemented with the relevant audit corrections.

Process qualifications reflect the changes in the quality of working processes and the current state reached as a result of the measures during the year. The change in quality of processes indirectly affects the estimated risk values through changing the probability of loss events shown in the operational risk matrix.

- During the evaluation of the qualifying factors, the business units also include the effect of the current quality of risk management tools on the KRIs.
- Internal Audit supervises and may modify the qualifications on the basis of its experience. It may supervise other data as well: the checking of various risks localised in the working processes and the values of potential losses in light of EI and actual loss data. It may supervise the impact of potential reputational damages and identify the potential shortcomings of the loss database based on the known loss events and loss data.

Elements of risk management monitoring:



5. The importance of comprehensive risk management

The comprehensive risk assessment process obviously involves each business unit.

Due to its novelty, the lack of experience and the lack of comparability with other central banking partners, the results of the assessment are probably not accurate enough; further analysis, data collection and development of the methodology should be carried out. In the present state of the work, however, we can already report about the following achievements:

- the process of self-assessment makes the business units think over their risks, therefore it fosters risk awareness in general while serving the purpose of prudent operations at the same time
- the operational risk map provides a comprehensive overview of the extent and location of these risks and this way risk management may be carried out on a uniform basis (for other risks as well, by extending the matrix), and it may also be used for preparing the annual audit plan
- the preparation of a clear set of standardised working processes helps the work of several business units in the field of internal regulation, quality management, planning, process expense calculation, controls and audit
- useful experience is gained by setting up the operational risk assessment system according to the Basel II guidelines, although no capital requirement applies to us. International practice can be tracked as several other central banks are known to be dealing with the issue. Moreover, our own experience may help us to better understand the work that commercial banks are doing in line with the Basel II requirements.

Table 1

Financial risks	**Operational risks**				**Business risks**
Credit, Market, Liquidity	People	Processes	External events	Systems	Strategic, Management

		Operational loss event types									
		External fraud	**Internal fraud**	**Execution delivery & process mgmt**	**Clients, products & business practises**	**Employment practices and work-place safety**	**Damage to physical assets**	**Business disruption and system failures**		**Total**	**Priority of working processes (qualified data)**
Set of standardised working processes							K	K		Σ	
			K				K			Σ	
				K			K			Σ	
						K	K			Σ	
							K			Σ	
Total			Σ	Σ		Σ	Σ	Σ		ΣΣ	

		Characteristic operational risk management tools						
Phases of operational risk management	Prevention	Protection Internal regulations	Internal regulations, Protection	Internal regulations, Quality mgmt.	Internal regulations	Internal regulations, Protection	Protection	Protection
	Managing emergency situation	Prompt intervention (+communication)	Prompt intervention (+communication)	Prompt intervention	Prompt intervention (+communication)	Prompt intervention	BCP (+evacuation)	BCP, DRP
	Preliminary measures for damage compensation schemes					Insurance	Insurance	

Table 2

Operational loss event type classification

Event-type categories (Level 1)	Event-groups (Level 2)	Loss events (Level 3)
Internal fraud (involving at least one internal party)	Unauthorised activity	transactions intentionally not reported (no report or documentation)
		unauthorised transactions (with monetary loss on the bank's side)
		intentionally mismarking of position, changing data
	Theft and fraud	fraud/credit fraud/worthless deposits
		theft/extortion/embezzlement/robbery
		misappropriation of assets, malicious destruction of assets
		forgery (involving at least one internal party)
		account take-over/impersonation/etc.
		bribes, kickbacks
External fraud (involving only third parties)	Theft and fraud	theft/robbery
		forgery (involving only third parties)
	Systems security	hacking damage
		theft of information (with monetary loss)
Employment practices and workplace safety	Employee relations (unlawful)	unlawful procedures requiring individual or group compensation (e.g. employment, termination, agency relations, contracts), discrimination
	Safe environment (health, physical safety)	losses due to lack of physical safety or due to general liability events (personal injuries, accidents, attacks, natural disasters)
		employee health and safety rules events
Clients, products and business practices (improper business practices)	Disclosure and fiduciary	customer disclosure violations (wrong, misleading or incomplete wording of conditions/regulations), failure to update them
		fiduciary breaches, misuse of confidential information
	Improper business or market practices	money laundering
		improper trade/market practices
	Product flaws	model errors, product defects, application of wrong structure
	Improper behaviour towards clients	failure to investigate client per guidelines
		exceeding client exposure limits
Damage to physical assets	Natural disasters or other events	natural disasters, breakdowns
		acts of violence (terrorism, vandalism – excluding robbery)
Business disruption and system failures	Extraordinary events arising from system failures	disruption due to hardware
		disruption due to software
		disruption due to telecommunications system
		disruption due to other failures (e.g. utility outage)

Event-type categories (Level 1)	Event-groups (Level 2)	Loss events (Level 3)
Execution, delivery & process management (inadequate processes)	transaction capture, execution and maintenance	miscommunication
		data entry, maintenance or loading error (for all working processes)
		missed deadline or responsibility
		model/system disoperation (wrong or outdated management)
		accounting error, entity attribution error
		misperformance of payments or services, payment processing errors
		improper maintenance of reference data
	Monitoring and reporting	failed mandatory reporting obligation (internal or external)
		inaccurate external report
	Customer intake and documentation	improper handling of clients' and legal documents (missing)
	Customer/client account management	negligent loss or damage of client assets
	Trade counterparties	non-client counterparty misperformance
	Vendors and suppliers	vendor disputes

Table 3

No	MNB working process structure (rows marked with Arabic numbers)
A	Function: **INVESTMENT BANKING**
I	Business line: **Trading and sales**
I/a	Activity: **Sales**
1	Settlement of coupons and notes unclaimed for payment until the end of the presentation period
I/b	Activity: **Treasury**
2	monitoring foreign currency position and transactions among nostro accounts
3	paying the instalments of medium-term and long-term interbank and syndicated loans taken up by the MNB
4	deposit transactions
5	spot transactions
6	forward transactions
7	swap transactions
8	repo transactions
9	security lending
10	futures transactions
11	option transactions
12	bond transactions
13	listing of foreign exchange rates
14	determining the BUBOR
15	deposit tenders
16	establishing and maintenance of the limit system
17	determining MNB's open currency position
18	working out and publishing the conditions of MNB HUF and foreign exchange market transactions
B	Function: **BANKING**
I	Business line: **Retail banking**
I/a	Activity: **Retail activities**
19	cash deposits and withdrawals of account holders
20	interest payments tied to KVH Rt bonds
21	changing banknotes and coins
22	processing the cash flown back to the Bank
23	safekeeping cash
24	safekeeping, managing and circulating the precious metal stock of the bank (rods, blocks, non-legal tender precious metal coins, legal tender commemorative coins)
25	organising transportation of cash
26	lending to employees
II	Business line: **Commercial banking**
II/a	Activity: **Commercial banking activities**
27	foreign currency guarantees (received, given, reciprocal)
28	export-import letters of credit
29	documentary collections
30	refinancing loans
III	Business line: **Payment and Settlement**
III/a	Activities: **Services to clients**
31	working out and publishing business conditions for bank accounts, HUF and foreign exchange settlements
32	opening, closing HUF and foreign currency accounts and data maintenance
33	settlement of interest relating to HUF and foreign currency accounts, periodical settlement of commission and other account keeping jobs
34	transfers within the interbank settlement system
35	collection orders within the interbank settlement system
36	settlement of cash transactions carried out with the intermediation of the Hungarian Post Ltd
37	clean payments
38	cheque processing

IV	Business line: **Agency services**
IV/a	Activity: **Custodian services**
39	custodian services
IV/b	Activity: **Corporate agency**
40	taking part in the preparation of international borrowing or bond issue of the sovereign issuer
C	Function: **CENTRAL BANKING**
I	Business line / Activity: **Emission**
41	projection of banknote and coin needs, working out production plan and production and stocking policy
42	working out withdrawal programme
43	settlement of withdrawal gain
44	working out issue programme of commemorative coins, managing commemorative coins
45	outplacement of cash
46	preparation of professional opinion on faked and suspicious Hungarian and foreign banknotes and coins
47	concerning non-negotiable and withdrawn money, destruction of banknotes and selling the material of coins
II	Business line / Activity: **Monetary policy**
48	creating the exchange rate regime, defining and publishing the MNB base rate, publishing the HUF refinancing, deposit and credit interest rates connected to the base rate
49	working out the regulations for minimum reserve requirement
50	calculation of the minimum reserves, determining the interest rates and taking sanctions unless the minimum reserve requirement is properly fulfilled
51	preparation of daily liquidity projection, monitoring liquidity
III	Business line/Activity: **Securing financial stability, central banking supervision**
52	LOLR: emergency liquidity loans
53	rating domestic banks
54	regulation and supervision of the Hungarian payment system
55	inspecting credit institutions, other financial enterprises, non-financial enterprises and money processing firms
56	licensing
IV	Business line/Activity: **Statistics, data supply, reports, publications**
57	statistical reports, data supplies
58	preparation of publications and reports
D	Function: **SUPPORTING AND SUPPLYING**
I	Business line/Activity: **Accounting, finance, controlling**
59	regulatory tasks: accounting policy, creation of ledger and analytical chart of accounts
60	keeping ledger accounts
61	keeping record of financial assets (investments), tangible and intangible assets, taking an inventory
62	record of buyers and suppliers, financial settlements
63	making provision, writing off depreciation/amortisation
64	preparation of MNB's Balance Sheet and Profit and Loss Statement, supported by inventory
65	preparation of MNB's tax return, settlement of tax liabilities
66	controlling activity
II	Business line/Activity: **Property services**
67	maintenance and operation of the building and related services
68	room management
69	travel arrangements
70	representation
71	procurement of material and assets needed for ensuring general working conditions (including telecommunication and labour protection), procurement of related services, inventory management, rollout
72	procurement and operation of the fleet
73	implementation of key (complex) capital expenditure projects
74	ownership representation
75	procurement of special emission tools, material and related services

76	IT procurement, storage
77	procurement of equipment and services needed for the development and operation of bank security systems
III	Business line/Activity: **Bank security**
78	organising the Bank's security system
79	assessment of operational risks, taking care of preventing or handling emergencies
IV	Business line/Activity: **IT**
80	network and system supervision, system administration, system security, access authorisation management
81	system operation and maintenance
82	development of IT systems
83	IT change management
V	Business line/Activity: **Human resource management**
84	planning and controlling of labour and labour-related costs
85	training
86	labour-related tasks
87	remunerations, social security, payroll
88	allotments
VI	Business line/Activity: **Administration and legal tasks**
89	working out the standard texts of decrees and contracts
90	representation of MNB in litigations and vis-à-vis authorities
91	preparation and harmonisation of laws
92	corporate affairs
93	operation of the system of internal regulations
94	file management
VII	Business line/Activity: **Communications**
95	external communications/information supply
96	publications
97	on-line communications
98	operation of libraries
99	banknote and coin collection, guarding, purchasing, changing the objects of the Museum of Bank History, exhibitions (Visitor Centre)
100	donations and sponsoring
101	translations and interpretations
102	internal programme management
103	information relating to international organisations
VIII	Business line/Activity: **Audit**
104	internal audit

Figure 1

Operational risk assessment model

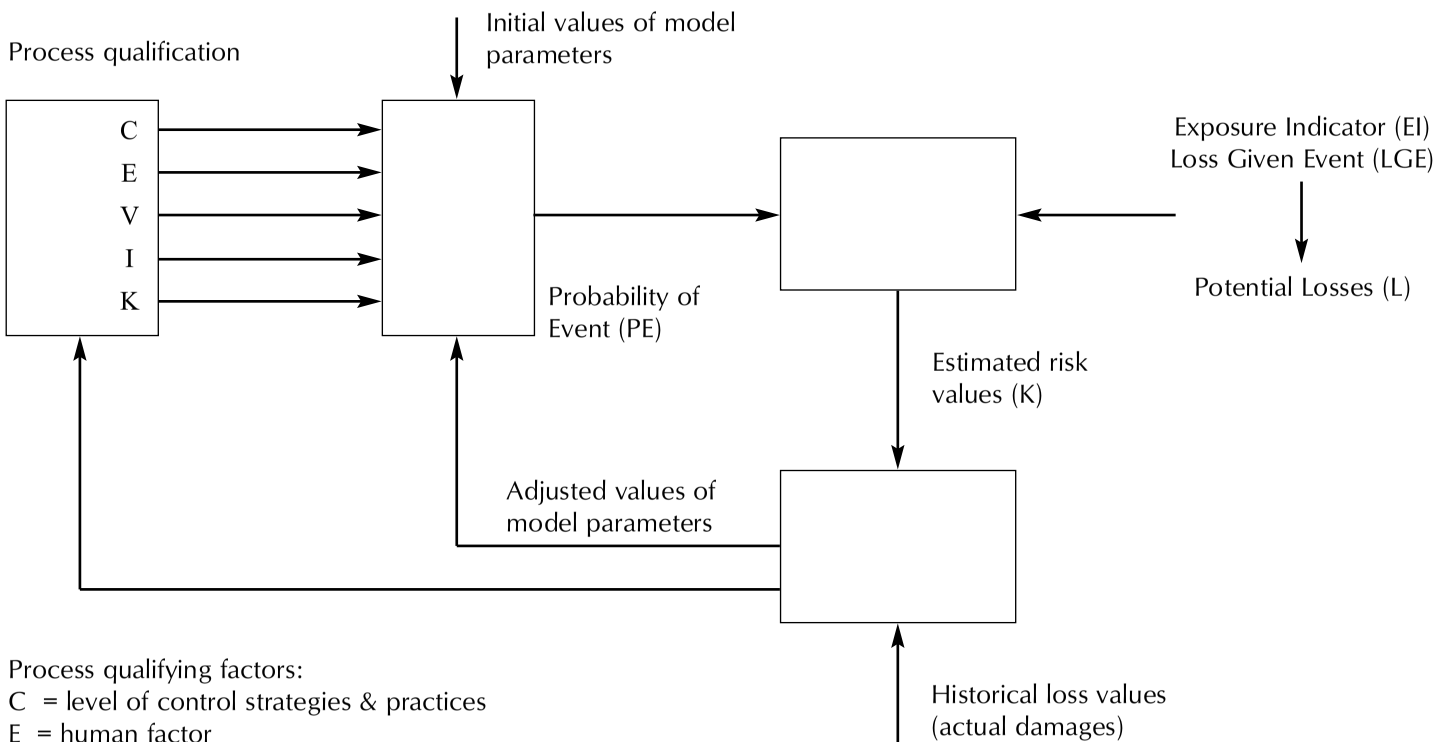
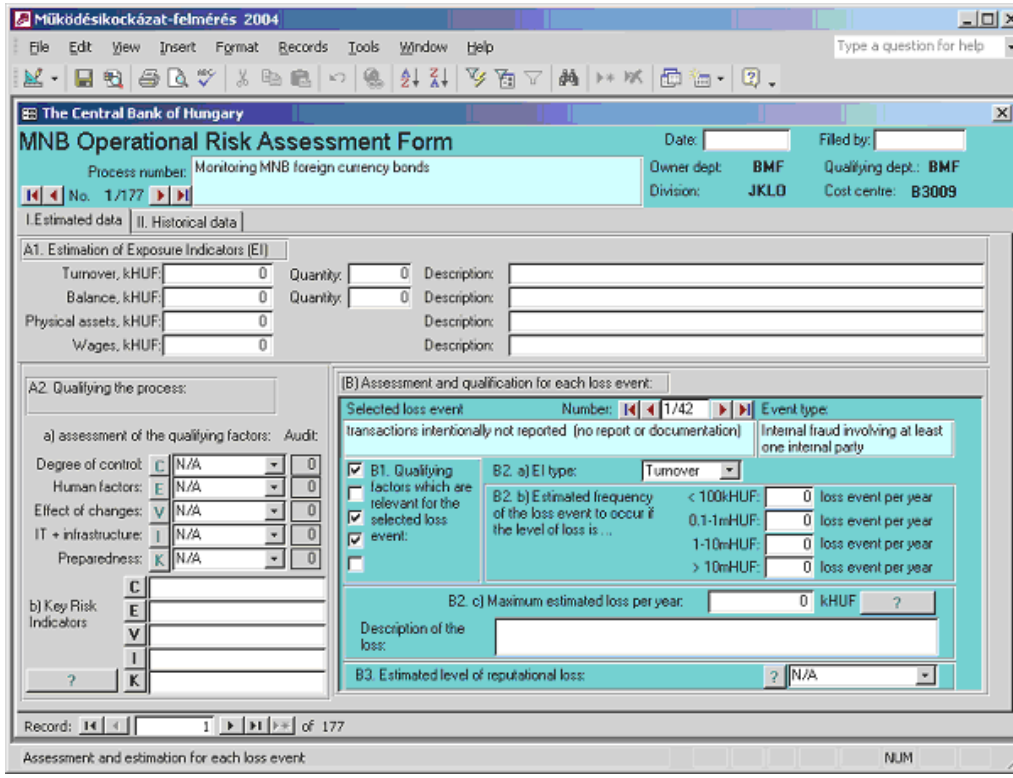


Figure 2


Működésikockázat-felmérés 2004
File Edit View Insert Format Records Tools Window Help
Type a question for help
The Central Bank of Hungary
MNB Operational Risk Assessment Form
Date:
Filed by:
Process number:
Monitoring MNB foreign currency bonds
No. 1/177
Owner dept: BMF
Division: JKLO
Qualifying dept.: BMF
Cost centre: B3009
I.Estimated data
II. Historical data
A1. Estimation of Exposure Indicators (EI)
Turnover, kHUF:
Balance, kHUF:
Physical assets, kHUF:
Wages, kHUF:
Quantity:
Description:
A2. Qualifying the process:
a) assessment of the qualifying factors:
Audit:
Degree of control:
Human factors:
Effect of changes:
IT + infrastructure:
Preparedness:
N/A
b) Key Risk Indicators
(B) Assessment and qualification for each loss event:
Selected loss event
Number:
1/42
Event type:
transactions intentionally not reported (no report or documentation)
Internal fraud involving at least one internal party
B1. Qualifying factors which are relevant for the selected loss event:
B2. a) EI type:
Turnover
B2. b) Estimated frequency of the loss event to occur if the level of loss is ...
< 100kHUF:
0.1-1mHUF:
1-10mHUF:
> 10mHUF:
loss event per year
B2. c) Maximum estimated loss per year:
kHUF
Description of the loss:
B3. Estimated level of reputational loss:
Record:
of 177
Assessment and estimation for each loss event
NUM

Assessing and Managing Operational Risks at the Magyar Nemzeti Bank
MNB Occasional Papers 32.

Print: D-Plus
H–1033 Budapest, Szentendrei út 89–93.