RISK MANAGEMENT
WORK GROUP (TASK FORCE)

METHODOLOGY

FOR RECORDING AND MONITORING

OPERATIONAL RISK IN BANKS

Belgrade, September 2006

Association of Serbian Banks
RISK MANAGEMENT WORK GROUP (TASK FORCE)

METHODOLOGY FOR RECORDING AND MONITORING OPERATIONAL RISK IN BANKS

I Basic Criteria and Principles

1. In the process of elaborating Methodology for Recording and Monitoring Operational Risk in Banks (hereinafter referred to as: Methodology), Task Force was well aware and mindful of the obligation prescribed for banks by the Banking Law and the appurtenant regulatory framework[1] "to identify and record such losses" and thereupon inform the National Bank of Serbia "of the losses incurred as a consequence of the operational risk, as well as those losses that may be incurred therefrom, and which are in excess of 1% of the bank capital".

2. Task Force was also bearing in mind that the manner of monitoring of the operational risk, as prescribed by the regulatory framework (8 lines of operation) and identification of business events containing operational risk exposure, have been taken over from the Basel 2 Accord.

   Such an approach was qualified as a very good starting point, when bearing in mind **the importance of standardisation of the risks definitions and identification procedures for the building up of comparable databases at the level of the system in general,** but also in a broader context, **and also that the process of formation of a database,** relevant for successful risk measurement, **is a long process** (taking a minimum of 3 years).

3. In the light of the above stated, Task Force, when elaborating this Methodology, followed the recommendations of the Basel Committee, with a view that these recommendations represent the very core of the most advanced knowledge and experience in the field of recording, monitoring and measuring operational risks.

[1] Decision on Risk Management ("Official Gazettee of the Republic of Serbia", No. 57 of 30 June 2006)

4. This Methodology **is not mandatory for banks**, but only offers an optional choice. Nevertheless, Task Force wishes to draw the attention to the two significant instances when speaking of this type of risk:

    - **the importance of standardisation of definitions (**allowing all the banks to identify those business events that result in losses caused by operational risks and record them in the identical categories) **for purpose of correct risk measurement**, but also **for comparability of data** between banks themselves, and

    - **the importance of correct approach from the very beginning** (allowed by the recommendations of the Basel Committee), not only for the purpose of measurement and comparability of data, but also for **lowering costs of monitoring** these risks in banks.

5. Task Force had examined carefully specification of events that may cause operational risk exposure, proposed in the Basel 2 Accord, and elaborated it further and supplemented, but also it had coded the specification for purpose of an easier monitoring.

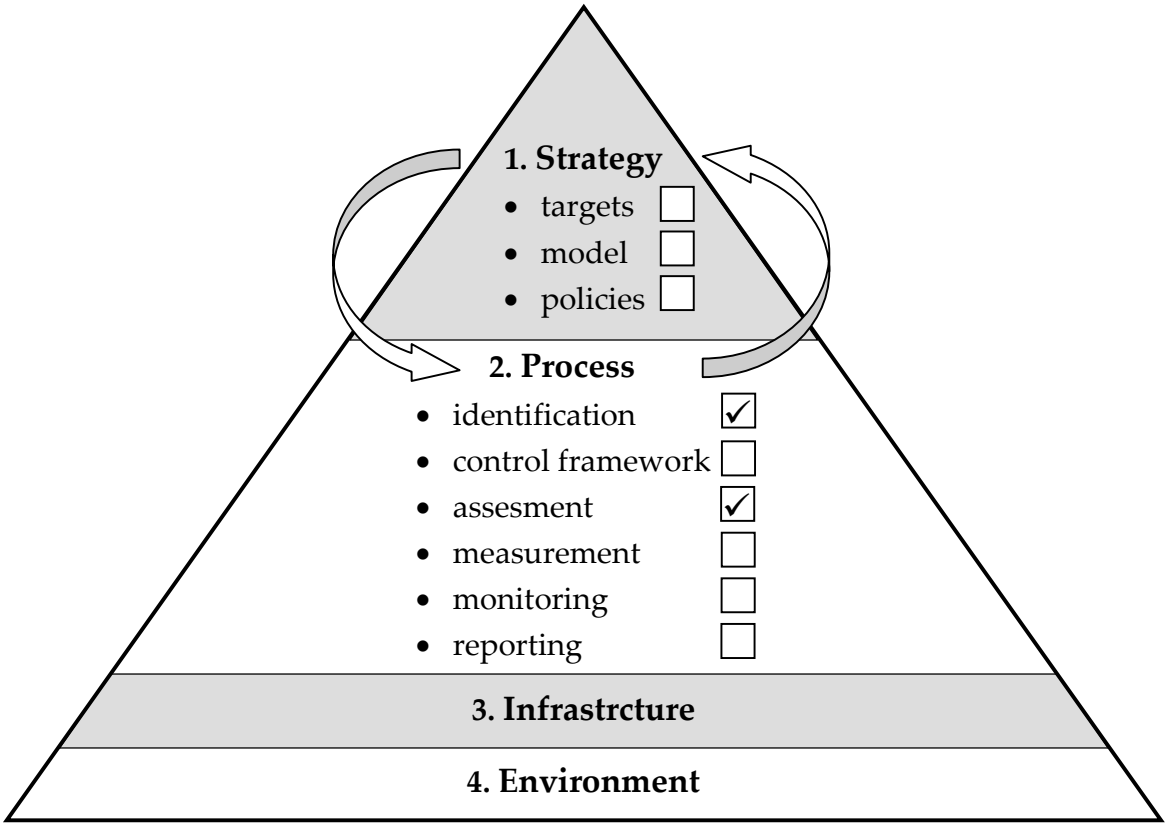
6. Mindful of the fact that there is an extremely short period of time for the realisation of this work, the proposed solutions serve as basis on which it is possible to **start with a uniform monitoring of this risk.**

    Task Force is well aware of the complexity of this task, but also of the fact that what is involved here is a process, and not a single assignment that can be accomplished in a single timeframe. In this sense, Task Force shall continue to work on the upgrading of these solutions, and shall keep all the member-banks of the Association informed of its progress report.

7. Task Force shall keep a follow-up on the results of application of the Methodology in practice. On the basis of return information received from the banks, periodically – every six months – it shall examine the need for its upgrading and adjustment to the realistic demands in practice, and shall inform all the banks accordingly.

II The place of Methodology within the operational risk management framework

1. Mindful of the definition of the term designating operational risk, the framework for operational risk management consists of four segments:



2. The present day actual obligation of banks prescribed by Law is defined as an obligation of banks to set up strategies, but also as **an activity in the first phase of the operational risk management process – identification of the source and recording of losses caused by operational risk.**

Tools: granulated operational risk mapping.

3. The proposed Methodology recommends identification of the operational risk and recording of losses from the operational risks, as follows:

   - along the lines of operation (see Appendix 1 – Mapping of operational lines);
   - according to the identified events that may cause operational risks and losses (granulated mapping) – see Appendix 2 – Matrix for classification of events that may cause operational risks and losses;
   - according to the causes (see Appendix 3 – Matrix of events that may cause operational risks and losses, per types of causes).

4. Continuous recording of data over a certain time horizon, by applying this Methodology, will allow formation of a database that shall be suitable for the following:

   - formation and strengthening of the management awareness of the multilayered level of organisation and the need for the data on accumulated losses to be unified into an aggregate picture of the total operational risk exposure;
   - empirical analyses and operational risk assessments; and
   - quantification of the operational risk exposure of the bank – measurement (that will be an obligation of the banks to perform in some forthcoming period, and a necessary requirement for it is the formation of a solid database).

III Mapping of operational lines

1. Methodology envisages identification of the operational risk source and monitoring of losses caused by operational risk, along eight lines of operation (Appendix 1 – Mapping of operational lines)[2].

2. Instruction[3]:

- All bank operations must be mapped within the proposed eight lines of operation;
- Any banking operation or a non-banking activity which explicitly can not be mapped within the proposed eight lines of operation, and represents an additional work to the main task which belongs to some of the operational lines from the proposed Framework, must be located within the line of operation where the main task belongs.
- Mapping of tasks within the operational lines must be clearly documented.
- For new tasks the association with one of the operational lines must be documented.
- Senior management will be responsible for the mapping process.
- Mapping process must be the subject of an independent auditing.

IV Matrix of events that may cause operational risk exposure and losses

1. Granulated mapping of the operational risk sources and losses that may occur on that basis, represent the matrix of the events that may cause operational risks and losses (Appendix 2). This matrix recognises the following:

[2] Mapping of operational lines was taken over from the Basel 2 Accord.
[3] Recommendations given in the Instruction are harmonised with the recommendations of the Basel Committee.

- Seven basic categories of events (Level 1)
- Sub-categories – further elaboration of business situations that may be classified within the main categories (Level 2), and
- Column with coded groups of events (Level 3) for an easier recording and monitoring.

V Recording of operational risk <u>according to causes</u>

1. Methodology envisages also a third level of monitoring operational risk according to causes (Appendix 3 – Matrix of events that are the sources of operational risk according to types of causes).

VI Database on operational risks

1. Mindful of the obligation of banks defined in the regulatory framework of the National Bank of Serbia, but also of the very substance of the term operational risk that is much broader, Task Force compiled a proposal for the elaboration of a database on operational risks (Appendix 4), which contains **minimum of data** necessary for recording and monitoring of the operational risks in banks. It combines together monitoring of operational risks along the operational lines, identified events causing operational risks and losses, according to events which are assessed as potentially conducive to operational risks yet are difficult or impossible to quantify, according to the type of loss/profit, and according to the types of causes of operational risks.

2. If the bank should wish to expand this database and monitor operational risk according to some additional and other criteria (types of consequences caused by operational risks, etc.) they are free to do so.

VII Table survey

Tables given from 1 to 4 (Appendix 1 to 4) are a component and integral part of this Methodology.

VIII Basic notions

Basic notions and terms used in this Methodology are defined as follows:

1. **Operational risk**. The broadest recognised definition of operational risk was published, for the first time, at Robert Morris Associates et. al. in the year 1999: "Operational risk is the risk of a direct or indirect loss caused by inadequate or unsuccessful internal procedures, human factor or system, or caused by external events". This definition was accepted by the Basel Committee but exclusive of the determinants "direct or indirect loss", and the definition of the Basel Committee is the basis for the definition of operational risk given in our regulatory framework[4].

   Definition of operational risk excludes reputational and strategic risks, but includes regulatory (legal) risk.

   Comprehensive coverage of the definition with respect to risk categories is significant for the formation of a framework for operational risk management (see picture on page 3) in the context of successful organisation of the operational risk management process and a uniform approach within the bank itself.

   Definition is primarily based on the operational risk causes, which served as basis for developing in practice of a complex approach to the operational risk, which differentiates between the causes of operational risks, actual events that are producing operational risks and losses, achieved profit/loss effect, and types of consequences.

   Methodology envisages operational risk monitoring according to five categories – along the operational lines, identified events producing operational risk losses, according to the events assessed as potentially conducive to operational risks but which are hard or impossible to quantify, according to the type of loss/profit, and

[4] Operational risk is a risk of incurring negative effects on financial result and bank capital due to shortcomings in the work of staff employed, inadequate internal procedures and processes, inadequate information and other systems management in the bank, and due to unpredictable external events" – Article 23 of the Decision on Risk Management – Official Gazettee of the RS, No. 57/06.

according to the types of operational risk causes, **and defines this as the basis for formation of a minimum database**. (See Part VI and Appendix 4).

2. **Reputational risk** is the risk of influence of public opinion on the current and future earnings, and on the growth of capital in a bank. It is reflected on the ability of the institution to establish new business relations and offer services or to continue to maintain the existing business relations. This risk may expose an institution to financial loss, but also to the fall in volume of business.

3. **Regulatory (legal) risk** is the risk of losses arising from the uncertainty regarding consistent implementation of laws, appropriate regulatory framework, and contract clauses.

4. **Strategic risk** is the risk of realisation of business plans and strategies – introduction of new business lines, expansion of the existing services and strengthening of infrastructure. For purposes of mitigating strategic risk, management should use strategic planning.

5. **Risk identification** is identifying events that are or may become potential sources of operational risk. The broadest framework for identification of operational risk is given by the definition of operational risk, and the historical component in the formation of the database provides additional information on potential operational risk sources.

   The result of the identification process is the matrix which presents in detail the presence of operational risk in different jobs, processes or organisational units of the bank. (Appendix from 1 to 4).

   Risk identification, further to the monitoring of internal factors, also covers monitoring of external environment, as well as the movements in the banking sector.

6. **Risk assessment** is the process of qualitative evaluation of the operational risk exposure, success in its control and monitoring. Risk assessment also allows a qualitative assessment of potential weaknesses, what should be upgraded in the organisation of work, who is responsible for the occurrence of risk exposure/losses, and how to overcome the situation through an organisational plan.

Therefore, the assessment is based on qualitative evaluation and this phase in the process of operational risk management is in this respect different from the measurement, which represents a quantitative assessment of operational risk exposure.

Tools: Self-assessment

Operational lines are the points of operational risk and the carriers of profit or loss due to operational risk exposure. Managers of these operational lines are responsible for loss assessment made on the basis of the database, and for the results achieved.

Belgrade, September 2006

TASK FORCE
FOR RISK MANAGEMENT
of the
ASSOCIATION OF SERBIAN BANKS

1. Banca Intesa – Darko Popovic
2. Raiffeisenbank – Dusan Banicevic and Dragana Radakovic
3. HVB Bank Serbia and Montenegro – Jelena Vasic
4. Komercijalna banka – Zlatan Zivkovic
5. Kulska banka – Brankica Jovancevic
6. Association of Serbian Banks – Vesna Matic, M.Sci.

Permanent associates of the Task Force for operational risk:

1. Banca Intesa – Djordje Stojanovski, M.Sci.
2. Komercijalna banka – Miodrag Dzodzo
3. Banca Intesa – Zeljko Gajic

APPENDIX 1

MAPPING OF OPERATIONAL LINES

Level 1	Level 2	Operational line code	Activity Groups
Corporate financing	Corporate financing	101	Mergers and acquisitions, Primary securities issue, Privatization, Securitization, Research, Public debt financing (great yields) and Equity capital, Syndicated deals, Initial public offer (IPO), Secondary securities offer
	Public sector/Government financing	102	
	Merchant banking	103	
	Consultancy	104	
Trade and sales	Sales	201	Fixed revenues, Equity capital, Foreign exchange, Goods, Loans, Funds, Securities trading for own account, Placement and Repo deals, Brokerage, Debenture stocks and bonds, Brokerage deals in primary issue
	Role of market makers	202	
	Propriatary Positions	203	
	Treasury	204	
Retail operations	Retail banking	301	Lending to households and deposits, Banking services, Depo deals and real estate.
	Private banking	302	Private placements and deposits, Banking services, Depo deals and real estate, Investment consultancy
	Credit cards	303	Individual and Business credit cards
Commercial banking	Commercial banking	401	Design financing, Real estate, Export financing, Trade financing, Factoring, Leasing, Other placements, Guarantees, Bills of Exchange – drafts
Settlements and payments	External clients	501	Payments and collections, Money transfer, Clearing and Settlement
Agency services	Custody	601	Escrow, Deposit receipts, Securities lending, Corporate activities
	Corporate Agency	602	Agent for issue, and Agent for collection
	Corporate fund	603	
Assets management	Discretionary funds management	701	Forming of pools, Segregation, Retail funds, Institutional funds, Closed-ended funds, Open-ended funds, Private equity funds
	Non-discretionary funds management	702	Forming of pools, Segregation, Retail funds, Institutional funds, Closed-ended funds, Open-ended funds
Retail brokerage deals	Retail brokerage deals	801	Enforcement and Other services

APPENDIX 2

Matrix for classification of events that may cause operational risks and losses

Operational Risk Categories (LEVEL 1)	Sub-category (LEVEL 2)	CODE	LEVEL 3
1. Internal fraud and activities Losses caused by intentional activities or omissions which include at least one person working for the bank, or at the bank. It is important to have the presence of "intent" to make personal gains	**1.1. Unauthorized activities** Losses caused by law violations, breach of contract, internal rules and procedures	**10101**	Failure to report transaction (intentional)
		10102	Unauthorized transactions (money losses)
		10103	Erroneously conducted operational activities (intentional)
		10104	Poor determination and presentation of position (intentional)
		10105	Intentional manipulation with documents
		10106	Misuse of vested responsibility
		10107	Other
	1.2. Theft and fraud Losses caused by acts aimed at personal financial gain	**10201**	Fraud/credit fraud/forgery/ bribe/money laundering
		10202	Fraud/extortion, embezzlement/bank raid robbery/theft
		10203	Misappropriation of bank property (funds, valuables)
		10204	Malicious destruction (damage to bank property)
		10205	Other malicious and illicit acts (misuse of cheque, account take over, tax evasion)
		10206	Forgery
		10207	Insider trading (for personal gain)
		10208	Other

	1.3. Internal security system Losses caused by unauthorized access and use of information from the banking IT system, malicious manipulation, and damage or deletion of data, unauthorized use of IT system by bank employees	**10301**	Misuse of IT system
		10302	Manipulation of files and programmes
		10303	Inappropriate deployment of confidential data
		10304	Other types of computer crimes (hackers …)
		10305	Other
2. External fraud and activities Losses caused by intentional acts committed by third persons. "Intentional" and "malicious" concepts prevail here, thus what is included here are the acts of fraud and swindle, or misuse or evasion of laws and regulations, rules and bank policies.	**2.1. Theft and fraud** Losses caused by acts aimed at personal financial gain	**20101**	Forgery
		20102	Theft/fraud and swindle/break-in
		20103	Misuse of cheques
		20104	Fraud
		20105	Other
	2.2. External Security System Losses caused by unauthorized access or attempt to access banking IT system by third person, with the aim to manipulate/seize/damage data, i.e. bank resources	**20201**	Damage of application by hackers (penetrating firewall)
		20202	Unauthorized access to applications
		20203	Damage to Net Server (Web-Server, Mail-Server, Proxy-Server …) by hackers
		20204	
		20205	Invasion by computer virus and worms
		20206	Other types of computer crime (hackers, theft of information …)
		20207	Other
	2.3. Other intentional activities Losses caused intentionally by incurring damages to the firm but without personal gain for the damage perpetrator	**20301**	Vandalism
		20302	Damage of bank property
		20303	Other

3. Attitude towards employees and safety at work Losses caused by failure to apply labour laws and other regulations related to labour, employment, health care and social protection, and safety at work	**3.1. Attitude towards employees** Losses caused by violation of labour law provisions	**30101**	Compensations, benefits, matters of termination of employment (service)
		30102	Organized trade union activities (industrial action – strikes, picketing)
		30103	Other
	3.2. Security of work environment Losses caused by failure to apply laws and regulations governing health care and social welfare, and safety at work	**30201**	Physical injuries of employees
		30202	Health and safety of employees
		30203	Other
	3.3. Diversities and discrimination Losses cause by any form of discrimination of employees	**30301**	All forms of discrimination (gender, race, religion, age, nationality)
4. Clients, products and business practices Losses caused by unintentional or negligent failures to comply with professional obligations towards clients, or arising from the nature or structure of products	**4.1. Propriety, transparency, and confidentiality**	**40101**	Breach of data confidentiality
		40102	Breach of Code of Conduct
		40103	Violation of client's privacy
		40104	Non-transparency towards the client
		40105	Erroneous/unlawful/negligent use of confidential data
		40106	Unauthorized trading practices (aggressive sales)
		40107	Account manipulation in order to create fictitious operations
		40108	Other
	4.2. Inappropriate business or market practices	**40201**	Violation of anti-monopoly regulations
		40202	Market manipulations/unauthorized trading or market practices
		40203	Engaging in unlicensed activities
		40204	Insider trading (for the account of the bank)

		40205	Failure to comply with the regulatory framework in force
		40206	Client discrimination
		40207	Violation of anti-money laundering law
		40208	Other
	4.3. Errors in products and services Losses caused by errors in products/services/models, or errors in contracts	**40301**	Errors in model
		40302	Ambiguous or punitive contract clauses
		40303	Other
	4.4. Selection, sponsoring and client exposure Losses caused by errors in selection of clients, in analyses of clients' needs, or overstepping exposure limits	**40401**	Errors/Inadequacy/Unsuccessful selection and client interview (opposed to the written rules and procedures)
		40402	Overstepping client exposure limits
		40403	Other
	4.5. Consultancy Losses caused by disputes with clients arising from consultancy activities, if this activity is regulated by contract	**40501**	Disputes on execution of consulting activities/Complaints on information and consultancy services rendered by the bank
		40502	Other
	4.6. Accidents and general security Losses caused by accidents which are incurring damages or injuries to third persons	**40601**	Injuries suffered by clients inside the bank's premises
		40602	Damages or injuries caused to third persons by the bank's vehicles
		40603	Other
5. Damages caused to fixed property Damages caused to fixed property due to natural disasters and other events	**5.1. Natural disasters** Damages of fixed property (buildings, infrastructure …) and human losses due to natural disasters	**50101**	Damages of fixed property due to natural disasters (storms, tornadoes, frosts, floods, eruptions, earthquakes, landfalls and landslides)
		50102	Human losses caused by natural disasters

		50103	All costs and debts incurred because of suspension and reconstruction caused by natural disasters
		50104	Other
	5.2. Human factor caused disasters Damages of fixed property (buildings, infrastructure …) and human losses due to natural disasters	**50201**	Damages to fixed property due to human factor caused disasters (terrorism, wars, riots)
		50202	Human losses due to human factor caused disasters
		50203	All costs and debts incurred due to interruption and reconstruction caused by human factor (industrial action – strike, riots)
		50204	Other
	5.3. Political and legal risks Losses caused by political or legislative changes	**50301**	Changes in law, etc.
		50302	Political changes
		50303	Other
6. Interruption of operations and fall of the system Losses caused by unavailability/shortages/ inefficiency of IT systems/providers of public utilities and information services. Losses caused by poor functioning of hardware and software, structural inadequacy, telecommunication shortcomings, etc.	**6.1. Inadequacy, inefficiency, poor functioning or fall of the IT systems** Losses caused by technical problems of the systems: unavailability, inefficiency, fall or disruption in the IT system (hardware, software, telecommunications)	**60101**	Inaccessibility of applications
		60102	Inability to receive and send data
		60103	Faulty automatic data processing (inaccurate and incomplete data)
		60104	Inaccessible or untimely systemic data offer
		60105	Fall of the system (application, network …)
		60106	Other
	6.2. (Public services/Information) unavailability of providers Losses caused by external services and use of providers	**60201**	Fall of the system of public services (telephones, power supply, etc.)
		60202	Other

7. Process execution, delivery and management Losses caused by unintentional errors related to the management processes and/or support. Here are also included the relationships with business partners, clients and providers (suppliers)	**7.1. Process management, coverage and execution of transactions**	**70101**	Poor communication
		70102	Input of data, maintenance or errors due to overload
		70103	Missed deadlines or other obligations
		70104	Failure to complete other tasks
		70105	Accounting errors
		70106	Inoperability of the model/system
		70107	Shortcomings in collateral management
		70108	Failures in delivery
		70109	Safekeeping data
		70110	Other
	7.2. Monitoring and reporting Losses caused by delayed or inaccurate reporting (to the public, to the central bank) or imprecise external report	**70201**	Failures in mandatory reporting
		70202	Inaccurate external reports
		70203	Other
	7.3. Reception of clients and adequacy of documents	**70301**	Shortage of documents (incomplete client's file)
		70302	Unsigned or incorrectly filled-in document
		70303	Other
	7.4. Managing client account Losses caused by errors in managing client account	**70401**	Unauthorized account access
		70402	Inaccurate client data (incurred losses)
		70403	Losses incurred due to negligence or damage caused to client's funds
		70404	Other

	7.5. Business partners Losses caused by errors/delays in settling transactions by business partners	**70501** **70502** **70503**	Poor work of business partners Disputes with business partners Other
	7.6. Vendors and suppliers Losses caused by disputes (litigation) with/bankruptcy of vendors or suppliers	**70601** **70602** **70603**	Disputes (litigation) Poor work Other

GENERAL REMARK: Risk category "Other" in Level 3 of the Matrix must not be higher than 10% of the total losses of Level 2 in the corresponding sub-category.

If this is the case, it is necessary to inform the Task Force which will then examine the possibility of revision of Level 3 of the corresponding sub-category, with the objective of introducing a new risk category.

Such changes must always be done at the level of the banking system in general, in the function of standardisation and uniformity of recording events that may cause operational risks and losses.

APPENDIX 3

MATRIX OF EVENTS THAT ARE SOURCE OF OPERATIONAL RISK ACCORDING TO THE TYPE OF CAUSE

Cause		Event Category
A	Human factor	1.1 Unauthorized activities 1.2. Theft and fraud by employees 1.3. Internal security system 3.1. Attitude towards employees 3.3. Diversities and discrimination 4.2. Inadequate business or market practices
B	Processes	3.2. Work environment security 4.1. Propriety, transparency and confidentiality 4.3. Errors in products and services 4.4. Selection, sponsorship and client exposure 4.5. Consultancy 4.6. Accidents and general safety 7.1. Managing processes, coverage and execution of transactions 7.2. Monitoring and reporting 7.3. Reception of clients and adequacy of documents 7.4. Managing client account
C	Systems	6.1. Inadequacy, inefficiency, poor functioning or fall of the IT systems
D	External factor	2.1. Theft and fraud (by third persons) 2.2. External security system 2.3. Other intentional activities 5.1. Natural calamities 5.2. Human factor caused disasters 5.3. Political and legal risk 6.2. (Public services/information) unavailability of providers 7.5. Business partners 7.6. Vendors and suppliers

APPENDIX 4

OPERATIONAL RISKS DATABASE

Item No.	Event starting date	Input date	Book entry date	Event ending date	Organisa-tional unit	Operation line (Level 2 code)	Event type (Level 3 code)	Gross amount	Insurance collected	Otherwise collected	Net amount	Status (code)	Cause (code)	Type of loss/profit (code)	Event description	Measures proposed

NOTE:

1. Bank is free to determine the minimum threshold for recording operational risks, provided that it is recommended that this threshold should not be higher than the dinar counter-value of 1,000 EUR. Minimum threshold shall designate that the risk below this threshold shall not be recorded.

2. All data contained in the database should be expressed in a single currency - Task Force proposes that all the banks should apply EUR currency, in order to allow for the comparability of data, mutual exchange and a more precise measurement, once the banks have reached that phase. If a bank should wish to keep the database in original currency in which the losses were incurred, this may be done by introducing additional columns, with the obligation for the amounts presented in the original currency to be cross-rated according to the mean exchange rate of the National Bank of Serbia, and expressed in the EUR column.

3. The events that are assessed as potentially leading to the operational risks loss/profit, yet which are hard or impossible to quantify, should also be recorded in the database, provided a dash (-) is inserted in the columns designated for recording the amount of loss/profit and collections.

4. Hereinafter the Task Force is presenting necessary codes for filling-in of the columns in the matrix of the Operational Risks Database, which are intended to facilitate monitoring and recording according to these criteria.

Status	**Code**		**Cause**	**Code**		**Type of loss/profit**	**Code**
Open	1		Human factor	1		Loss	1
Under investigation	2		Processes	2		Operational profit	2
Completed	3		Systems	3		Loss avoided	3
Approved	4		External factor	4		Lost profit	4
Closed	5						