OPERATIONAL RISK IN INTERNATIONAL BUSINESS: TAXONOMY AND ASSESSMENT METHODS

Marinoiu Ana Maria
Bucharest University of Economics, Faculty of International Business and Economics, Piaţa Romană, 6, Bucharest, anamarinoiu@yahoo.com, 0722701525

The paper aims at presenting the classifications and the assessment methods for operational risk according to international regulations (ie. Basel 2), in the context of its importance as a managerial tool for international business. Considering the growing complexity of the organizational and operational structures of the multinational companies, it is of utmost importance to quantify a risk that may cause on the short run considerable damage to the profits and cash flows of the companies and even to its existence.

Key words: operational risk, theories, international business

JEL:G32

Organizations that may have focused a few years ago on delivering one or two similar products constructed in one location to a single, homogenous group of clients have evolved into true multinational enterprises. Nowadays, manufacturing may take place in a number of locations around the world, and in each location different styles and variations of the product line may be developed. Manufacturing competencies are kept distinct from the skills required to develop an efficient distribution capability. Distribution is also likely to be a multi-location activity, and in each location a variety of different channels may be employed to reach clients. With so many flexible issues, the management and control problem of a modern firm is enormously complex. One has to efficiently coordinate intelligent, motivated individuals, who in many cases represent the value of the organization, to execute an intricate and sophisticated process. These individuals must retain some scope for personal challenge and reward, while the organization overlays a structure for achieving stability and growth to ensure product quality, at the same time delivering a return on capital for the shareholders. All these factors constitute a varied range of potential risk sources, hence underlining the necessity for a risk management strategy for the companies involved in national and multinational activities. Another explanation as to why firms pursue risk reducing strategies in a risk management framework is presented in Amihud and Lev (1981), who argue that imperfect monitoring and contracting allow managers to take actions that are in their own best interest and not necessarily those of shareholders. A third interesting explanation, this time focused on operational risk, is that operational risk management optimises the loss versus control, as shown in the figure below.

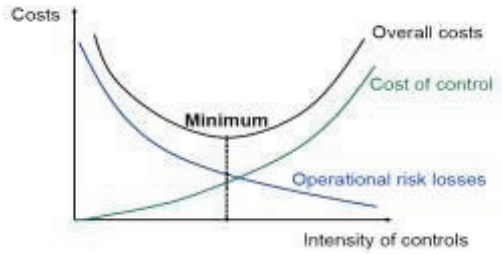
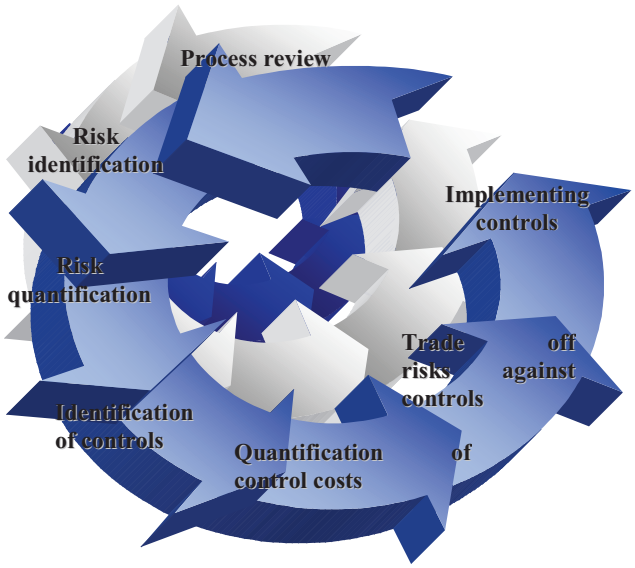


Figure 1The Optimization of loss versus control trade off by using operation risk management

Therefore, indicators quantifying risks from an objective point of view offer both managers as well as shareholders the opportunity to rely on simple and easy-to-use instruments in order to

determine a best-practice course of action. In practice, risk management methods fall into two major categories: risk adjusment and risk analysis (probabilistic risk analysis). The latter uses instruments and methods such as sensitivity analysis, probability analysis, decision-tree analysis, Monte Carlo simulation etc.

There are many examples of how an incomplete knowledge of risks can lead to inefficiencies or worse. Three broad classes of problems can arise from a failure to manage risk: (i) a potential compounding of unintended bets and uncompensated exposures to risk, (ii) unwarranted over-diversification or the reverse, concentration, and (iii) misallocation of resources. Hence, the management of operational risk requires a process of risk and control assessment, as presented in the figure below. The present paper deals with stages 2 and 3 in the scheme, presenting the classification and assessment methods for operational risks.



Classification of operational risks

In response to the growing awareness of operational risk and the need to manage it, the regulatory community is providing guidelines from defining operational risk to establishing guiding principles on the quantification of operational risk. Therefore, several competing classification schemes have become available in the operational risk services market.

The seven operational risk loss event groups recommended by the Basel Committee are:

1. Internal Fraud
2. External Fraud
3. Employment Practices & Workplace Safety
4. Clients, Products, & Business Services
5. Damage to Physical Assets
6. Business Disruption & System Failures
7. Execution, Delivery, & Management Process

The operational risk classification methodology proposed by Zurich IC2 lists five major risk classes and their associated subcategories.

1. People Risk:

- Employee Errors (general transaction errors, incorrect routing of transaction, *etc.*)
- Human Resource Issues (employee unavailability, hiring/firing, *etc.*)
- Personal Injury – Physical Injury (bodily injury, health and safety, *etc.*)
- Personal Injury – Non–Physical Injury (libel/defamation/slander, discrimination/harassment, *etc.*)

- Wrongful Acts (fraud, trading misdeeds, *etc.*)

2. Process Risk:

- Business Process (lack of proper due diligence, inadequate/problematic account reconciliation, *etc.*)
- Business Risks (merger risk, new product risk, *etc.*)
- Errors and Omissions (inadequate/problematic security, inadequate/problematic quality control, *etc.*)
- Specific Liabilities (employee benefits, employer, directors and officers, *etc.*)

3. Relationships:

- Legal/Contractual (securities law violations, legal liabilities, *etc.*)
- Negligence (gross negligence, general negligence, *etc.*)
- Sales Discrimination (lending discrimination, client discrimination, *etc.*)
- Sales Related Issues (churning, sales misrepresentation, high pressure sales tactics, *etc.*)
- Specific Omissions (failure to pay proper fees, failure to file proper report, *etc.*)

4. Technology:

- General Technology Problems (operational error – technology related, unauthorized use/misuse of technology, *etc.*)
- Hardware (equipment failure, inadequate/unavailable hardware, *etc.*)
- Security (hacking, firewall failure, external disruption, *etc.*)
- Software (computer virus, programming bug, *etc.*)
- Systems (system failures, system maintenance, *etc.*)
- Telecommunications (telephone, fax, *etc.*)

5. External:

- Disasters (natural disasters, non–natural disasters, *etc.*)
- External Misdeeds (external fraud, external money laundering, *etc.*)
- Litigation/Regulation (capital control, regulatory change, legal change, *etc.*)

A transference from one of these classification method to the other is possible, as presented by Alvarez in GARP (Global Association for Risk Professionals) studies.

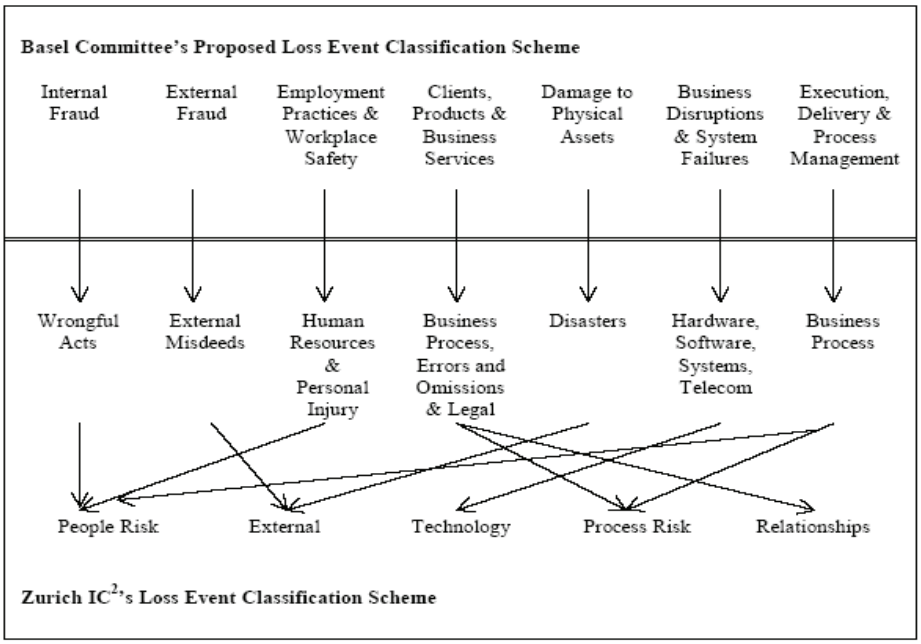


Figure 2 Mapping illustration between the Basel Committee's proposed operational risk event classification scheme and Zurich IC2 format. (Alvarez, 2002)

Methods for assessing operational risk

In literature, many authors support the risk analysis approach, emphasized by the increasing use of risk-analysis techniques. However, one reason for a wide-spread acceptance of risk analysis is that it is affected by the practical implementation methods.

There are several methods that may be used for assessing the level of operational risk that a company has to deal with. Each of these methods has its advantages, as well as its downfalls in terms of benefits for the company. For the control of the universe of operational risks, the risk measuring instruments complement and overlap each other, as shown in the figure below. In the following pages, some of these methods are briefly presented.

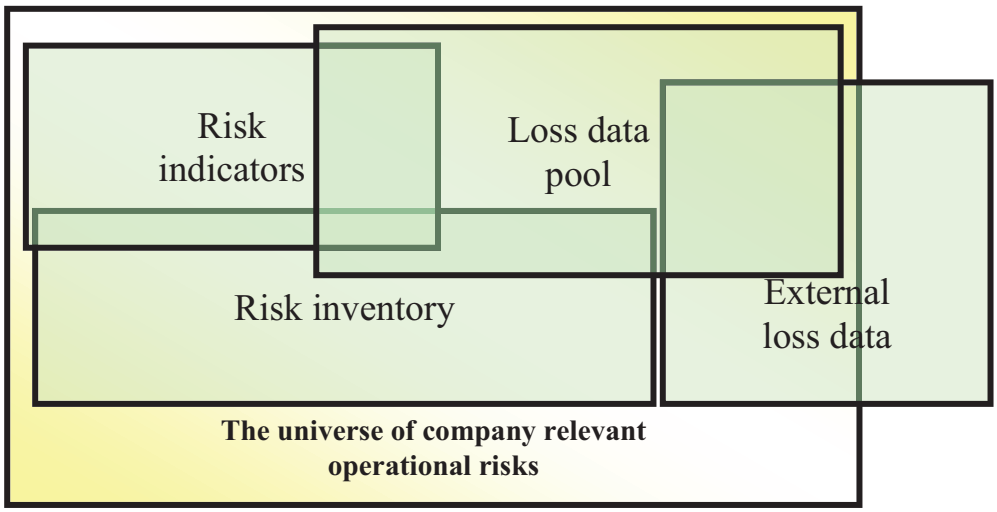


Figure 3: Risk measuring instruments, according to GARP (Global Association of Risk Professionals), 2001

1. Scalars

The first method is the use of simplistic business scalars (such as revenues, costs, assets, funds under management and volume of payments) to measure operational risks. This approach makes no attempt to explicitly measure differences in risk between units, as the scalars available for use are in many cases poor proxies for risk. The scalars may be, depending on structure of company, industry, legal requirements, and internal processes:

Indicators of human risk

- -Overtime
- -Fluctuation
- -Period of employment

Indicators of process risk

- -Degree of automation
- -Delays in transactions
- -Range and bearing of projects

Indicators of technological risk

- -Age of system
- -Degree of utilisation of system
- -Duration of breakdown

Indicators of product risk

- -Age of product
- -Number of products

-Product range and scale

2. Benchmarks

Under this approach, amounts of economic capital held by similar business lines in other banks are used to determine the appropriate amount of capital for each unit. This approach has the merit of being relatively quick and easy to apply, but it is a proxy measure rather than a real quantification. Moreover, benchmarks relate to companies with different products, different markets (particularly if they are overseas) and different internal processes. One of these benchmarks may be considered the Operational Value-at-Risk for the industry, a parameter that succeeds at eliminating some of the problems presented above.

$OpVaR_{ij}$ =	Probability of event	X	Loss given event	X	Operations exposure	X	Quality index

For any combination of business segment i and type of risk j, the following parameters need to be calculated:

-Probability of loss event, PE
-Loss given that event, LGE
-Operations exposure, OE
-Quality index, assumed to be independent

3. Statistical analysis

The statistical approach is faulty due to the poor quality and quantity of internal data available, especially when it is applied "bottom-up". The foundation of any thorough analysis of operational risk is data integrity and quality. If data are sparse, biased, and incomplete or flawed, the outcome of any analysis will be suspect at best; meaningless at worst. Because of this fundamental relationship between data quality and trustworthy results, the process of data gathering must be as diligent as the quantitative analysis. When categorizing operational risk loss data, the traditional approach is to group the loss events based on their causes.

Even more fundamentally, the statistical approach (using internal or external data) will not reflect recent changes in risk profile, either inside or outside the company. Another important issue is that the measurement of risk and allocation of economic capital, using a history of internally collected data, may act as something of a disincentive to collect the necessary data or record losses in a transparent fashion. Basically the statistical analysis, as well as the creation of a statistical model, is based on the scalars presented above, therefore, fundamentally flawed, due to their disadvantages. However, a statistical analysis, based on dynamic indications such as the OpVaR, as seen in rolling correlation with the other indicators of the company and industry, and in a matching set with its determining factors (after applying a factor analysis) may prove to be a method worthy of taking into consideration.

4. Scorecards

The use of operational risk "scorecards", composed of forward-looking risk indicators is another important method, used by several important companies. The scorecards can be used to allocate business units a pool of operational risk capital that has been calculated by other means (for example, by benchmarks or statistical analysis). The scorecard approach avoids many of the problems inherent in analysis of historical data, and can be much more forward-looking, by capturing the knowledge and experience of the experts who design the scorecards. However, the data collection problems are transferred to the collection of risk indicators, which can also suffer from quality issues. And the reliability of the output becomes quite dependent on the experts

employed to design the metrics and weightings within the scorecard. It is possible that a badly designed scorecard could produce results completely at dissonance with reality, intuition and the actual history of losses. The expert panels goes through a structured process of identifying the drivers for their risk category, and then forming these into questions that could be put on scorecards. Some of these questions ask for quantitative data (for example, staff turnover rates), others for qualitative judgments (such as the rate of change in different businesses), and still others are simply yes/no questions (such as indicating compliance with certain group policies). These questions were selected to cover drivers of both the probability and impact of operational events, and the actions that the bank has taken to mitigate them. The following few examples illustrate the range of scorecard questions:

-Fraud: What percentage of your unit's staff is on business growth/sales performance/profit performance-based remuneration?

-Process: What percentage of your unit's staff did not take 10 days' consecutive leave in the last 12 months?

-Personnel: Do you have a formal and documented business continuity plan, which addresses personnel failure (e.g., the non-availability of key personnel)?

The application of a mix of the methods presented above may have the following three stages. Firstly, calculating the total operational risk economic capital for the group (using a combination of statistical methods and benchmarks). Second, allocating this total between the different categories of operational risk (e.g., fraud, IT, personnel, legal, compliance, etc). Third, allocating the capital for each category to individual business units using the results of a scorecard particular to that category, and a volume scalar also selected for that category (e.g., number of staff for personnel risks). Most importantly, the capital allocations to business units can then be disconnected from each other and scaled according to changes in the individual unit's risk scores and scalars. This is important because it stops the capital allocation process being a zero-sum game, where a unit might be penalized as a result of other units improving their scores rather than through deterioration in the unit's own profile. Instead, each unit is given strong incentives to manage and reduce its operational risks, independent of actions taken by any other unit, since the reduced risks would subsequently be reflected in reduced economic capital allocations.

References

1. Álvarez, G – "A Rigorous Way for Quantifying Data", GARP Risk Review, Issue 4 Dec 01 / Jan 02
2. Basel Committee on Banking Supervision: "Consultative Document Operational Risk", 2001
3. Basel Committee on Banking Supervision: "QIS Operational Risk Loss Data", 2001
4. BIS, 2001. "Consultative document: operational risk", 2001.
5. BIS, 2001. "Working paper on the regulatory treatment of operational risk", 2001
6. Bookstaber, R - "Risk Management in Complex Organisations", Berkeley Finance Symposium, 7. The Association for Investment Management and Research, 1999
8. Chernobai A, Menn C, Rachev ST,Truck S – "Estimation of Operational Value-at-Risk in the
9. Presence of Minimum Collection Thresholds", 2005
10. Cruz, M. G – "Modeling, Measuring and Hedging Operational Risk". John Wiley & Sons, New York, Chichester, 2002.
11. Davis, E. – "Operational risk: Practical Approaches to Implementation".Risk Books, London. 2005
12. http://www.bis.org
13. http://www.gloriamundi.org/
14. http://www.opriskandcompliance.com/
15. Jorion, P. – "Value-at-Risk: the New Benchmark for Managing Financial Risk", 2nd Edition. McGraw-Hill, New York, 2000.

16. Jun Pan, Duffie D – “An Overview of Value at Risk”', Journal of Derivatives , Spring 1997, 7-49
17. Kloman, HF – “Integrated Risk Assessment”, at www.riskreports.com
18. May, D – “Do Managerial Motives Influence Firm Risk Reduction Strategies?”, Journal of Finance, Vol. 50, Issue 4, 1995
19. Moscadelli, M. – “The modelling of operational risk: experience with the analysis of the data collected by the Basel Committee”, 2005.
20. Zurich IC Squared, www.ic2.zurich.com