NEW TRENDS REGARDING THE OPERATIONAL RISKS IN FINANCIAL SECTOR

Assoc. Prof. Ph.D. Laura Giurca Vasilescu
University of Craiova
Faculty of Economics and Business Administration, Romania

Abstract: Risks, especially "operational risks" are part of corporate life, they are the essence of financial institutions' activities. Operational risks are complex and often interlinked and have to be managed properly. Today, there is more pressure to avoid operational risks while continuing to improve corporate performance in the new environment. The operational risk management of the future has to be seen in the wider context of globalization and Internet-related technologies. The two major future drivers - globalization and Internet-related technologies - will challenge the firms from financial sector to take on additional and partly new operational risk.

Key words: operational risk, financial sector, models, trends

1. Introduction

Risk management has always been an explicit or implicit fundamental management process in financial services. Today, however, there is more pressure to avoid things going wrong while continuing to improve corporate performance in the new environment. Good risk management is a decisive competitive advantage. It helps to maintain stability and continuity and supports revenue and earnings growth.

Risk management is an obligation to stakeholders; diligent and intelligent risk taking is an "attitude" towards stakeholders. Despite all the progress in the quantification of risks, risk management will remain a blend of art and science. Quantified risk is seductive, but can be misleading or provide a false sense of security and therefore the imperfections have to be acknowledged.

Risk management is a daily struggle against uncertainty and a daily learning process. Risk management is not a program, but a process for which senior management and Board of Directors are increasingly called upon to ensure. New governance requirements are quite explicit about this responsibility. Good risk management is not only a defensive mechanism, but also an offensive weapon. Quality of leadership and governance is increasingly an issue of risk management. More and more the comprehensive, institution-wide strategy and tactics towards risk should be based on credible methodologies in order to identify, define, assess, reduce, avoid and manage risk.

Risk is uncertainty about a future outcome. The daily life of a human being is full of risks, especially "operational risks". Risk is part of corporate life; it is the essence of financial institutions' activities. A recognized risk is less "risky" than the unidentified risk. Risk is highly multifaceted, complex and often interlinked. While not avoidable, risk is manageable - as a matter of fact most banks live reasonably well by incurring risks.

2. Operational Risk in Financial Services

2.1. Operational Risk as part of Risk Management

The risks faced by a firm providing banking and insurance services are partly overlapping or interdependent (figure 1). The main challenge for risk management is to separate them in an intelligent way.

This separation exercise forms core risk classes for the daily management and quantification where possible and credible. To do this, the pragmatic management angle should be taken. The ability to use a common, uniform management technique based on the peculiar features of a risk class provides the rule for drawing the line to other risks.

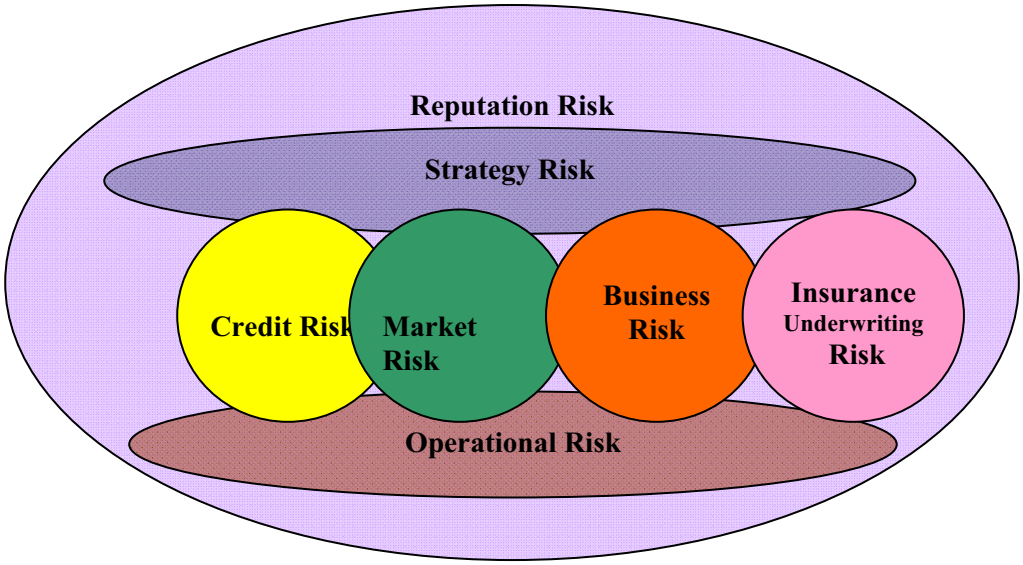

Figure 1: Overlaps between Risk Classes

Credit and market risks originate form outside the bank. The management of market and credit risks has made great progress as to its methodologies and quantification approaches, given the vast and reasonably reliable data and statistics. This does not mean that misjudgments as to the future are rare, but the approach is more empirically founded.

Contrary to market and credit risks, operational risks are usually not willingly incurred, often they are insignificant in an overall context. Also for reputation reasons, operational risks are avoided.

Operational risks are primarily institutional, internal, context dependent, incredibly multifaceted, often judgemental, interdependent, often not clearly discernible vis à vis e.g. market and credit risks and not diversifiable.

Having recognized the above, a suggested operational risk definition could be: "*Operational risk is the risk of adverse impact to business as a consequence of conducting it in an improper or inadequate manner and may result from external factors.*" This definition needs categorization: organization, policy/process, technology, human, external which in fact are the main five categories of operational risks:

a). *Organization*: risks arising from such issues as change management, project management, corporate culture and communication, responsibilities, allocation and business continuity planning;

b). *Policy and Process:* risks arising from weaknesses in processes such as settlement and payment, non-compliance with internal policies or external regulation or failures in products or client dealings;

c). *Technology:* risks arising from defective hard- or software, failures in other technology such as networks or telecommunications, as well as breaches in IT security;

d). *Human:* risks arising from failure of employees, employer, conflict of interest or from other internal fraudulent behaviour;

e). *External:* risks arising from fraud or litigation by parties external to the firm, as well as lack of physical security for the institution and its representatives.

Operational risks management is often close or parallel to quality management and, therefore, contributes to client satisfaction, reputation and shareholder value. These are some of the reasons why the definition, measurement and modeling of operational risks are so difficult to be done.

To understand the operational risks has always been a fundamental, if only implicit, management process. The novelty consists in the followings:

- the increased explicit awareness and consciousness of managers and senior management for operational risk issues;
- the explicit and analytical approach;
- the better awareness to gear an organization's risk profile towards those risks for which it has a comparative advantage in managing
- the pressure to allocate capital more consciously.

The risk management can add value and represent a valid business case in two dimensions:

◊ Control: independent risk assessment, compliance, business continuity planning, supervisory requirements, limits, progress reporting, corrections etc.;

◊ Shareholder value creation: efficiency, correct risk evaluation and pricing, rational economic capital allocation, reduction of regulatory capital, product enhancements, competitive strategic advantage, improved reputation, etc.

This dimension adds a further stage which treats operational risk more like a real business. Operational risk management also gets close to quality management, efficiency management and the concept of opportunity cost.

Naturally, the line between control and shareholder value creation is difficult to be drawn. Important is the direction to be chosen. Operational risk management, therefore, can move from one extreme to another one: crisis management → business continuity planning → compliance → shareholder and other stakeholder value enhancement. There are neither ready-made solutions, nor quick-fixes.

Implementing operational risk management implies the progression through the following four stages in figure 2:

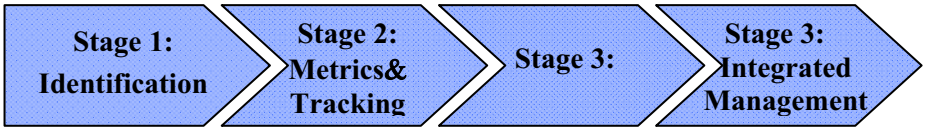

Figure 2: Stages of Operational Risk Management

1). The first stage *"Identification*" implies:
• data collection;
• prioritization of risks;
• significant business unit involvement;
• limited technology usage;
• significant use of manpower.
2). The second stage "*Metrics and Tracking*" implies:
• finding quantifiable means to track risks;
• creation of reporting mechanism;
• significant business unit involvement;
• investment in automated data gathering and workflow technologies;
• significant use of manpower.
3). The third stage "*Measurement*" implies:
• development and continuous refinement of modeling approach;
• creation of operational risk data;
• significant technology development effort;
• limited use of manpower.
4). The fourth stage "*Integrated Management*" implies:
• integration operational risk exposure data into management process;
• significant senior management involvement;
• management of operational risk exposures (e.g. insurance);
• investment in processes;
• limited technology or manpower required.

Mistakes and failures (for instance, operational risk losses) happen daily in every financial services organization and some are negligible, some more serious but very rarely they can be very grave.

With dramatically increased competition - also from non-banks - a successful operational risk management is crucial for survival. In the future, the market will be less forgiving of any colossal lapse. Reputation is increasingly also built on operational risk management skills.

Operational risk management is in fact good management and close to quality management. As management in financial services is dealing with people for people - in a continuous process and ever changing environment - there cannot be an easy answer or a simple model.

The general environment for financial services will continue to change dramatically. It will require for significant and continuous adjustments in the way enterprises do business and adapt their operations. As a result, operational risk will primarily be driven by: new products; product sophistication; new distribution channels; new markets; new technology; E-Commerce; business volume; new legislation; role of non-government; globalization; shareholder and other stakeholder; regulatory pressure; Mergers and Acquisitions; reorganizations; staff turnover; cultural diversity of staff and clients; rating agencies; insurance companies; capital markets, cultural diversity of staff and clients, faster ageing of know-how, rating agencies.

But operational risk and operational risk management are not only about risks and threats. Both are chances and opportunities as well. Therefore, the new approaches can solve many old problems.

2.2. Modeling Methods of Operational Risk

Regarding the quantifications or modeling method for operational risk there are a number of choices including:

- a qualitative assessment;
- a process mapping;
- a quantitative modeling.

The figure nr. 3 provide an overview of the methods at disposal - at least theoretically - to quantify and model operational risk.

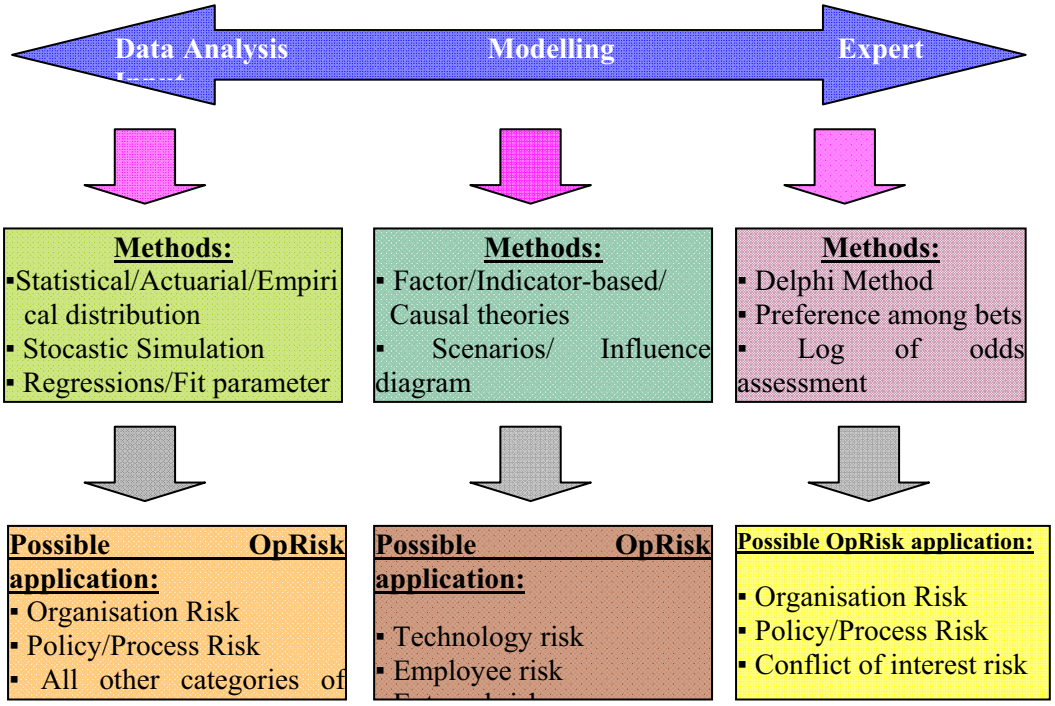

Figure 3. Modeling Methods of Operational Risk

The techniques presented under "Expert Input" (for example the "Delphi method" or the "Log of odds assessment") as well as the most simple forms of "decision trees" and "influence diagrams" are essentially qualitative assessment and process mappings.

The techniques presented under "Modeling" and "Data Analysis " (figure 3) is more quantitative by nature. Among these, there are the following methods:

a) The factor-derived or indicator-based quantification models.

These models apply causal factors to build a prediction of the level of risk. For example, they would use a combination of error rates, failed reconciliations, employee training expenditure, staff turnover, indicators of the IT system complexity, indicators for the quality of governance, etc. to project a level of operational risk. They tend to produce a figure for the relative future value of the causal factors on operational risk, but not necessarily of the operational loss amount. They are also considered to be only partially representative for operational risk causes.

The BIS has suggested an indicator-based quantification as a possible method for the quantification of operational risk and the corresponding regulatory capital allocation. The level of operational risk is identified by a multiple of a simple observable indicator or a combination thereof. Suggested indicators include: gross revenues, fee income, operating costs, managed assets or total assets adjusted for off-balance sheet exposures.

The BIS method is a factor/causal theory model simplified to its extreme. It assumes a linear link between the level of operational risk and business activity, thereby offering the advantage of being easily implementable. Empirical tests show that this assumption is not verified. But, the most important drawback of the BIS causal theory model is that an operational risk quantification based on exclusively measurable indicators is bound to produce incorrect and misleading approximations of operational risk. This is because the high context dependency of most operational risk elements makes qualitative, nonmeasurable operational risk aspects critical in determining its level.

The BIS method also bears the danger of creating perverse incentives. For example, lowering control related costs would save capital, but also raises the operational risk. Lowering fee income would save capital, but also crowd-out the regulated fee-income banking activities in favor of unregulated financial actors and thereby increase the systemic risk within the financial markets.

The drawback of relying exclusively on measurable indicators in factor/causal methods can be overcome by integrating qualitative aspects of operational risk. These methods could be particularly useful in top-down frameworks to gain insights in both, low and high frequency events. However, there is still a long way to go. Up to present times, the operational risk literature has remained nebulous about operational risk explanatory variables.

b) The statistical/actuarial or simulation based quantification models.

These models use actual loss data to construct representations of operational loss frequencies and severity in the form of statistical probability distributions. To do this, they require many data points and have to rely on the existence of complete operational risk databases.

Simulation-based quantification models are very popular in the literature on operational risk, particularly the actuarial inspired Monte Carlo simulation technique. The prime reason for this is that they allow filling the data gap prevailing in operational risk for low probability events.

For each operational risk category or sub-category these models generate a loss distribution. To do this - applying randomly generated inputs to the underlying risk distribution of an operational risk sub-category - thousands of hypothetical years are simulated, until a stable "empirical" loss distribution is produced. The process can also be scaled down to individual business lines; loss distributions for each of their relevant operational risk sub-subcategories can be generated. Interdependencies among operational risk elements can also be taken into account.

The outcome of this exercise (figure nr. 4) is familiar to market and credit risk specialists. But the present state of operational risk data does not allow for any backtesting of the correctness of the generated distribution. In addition, slight changes in the environment, due to the high context dependency of operational risk, will have a significant impact on the generated distribution. These would require reviewing the entire underlying simulation setting.

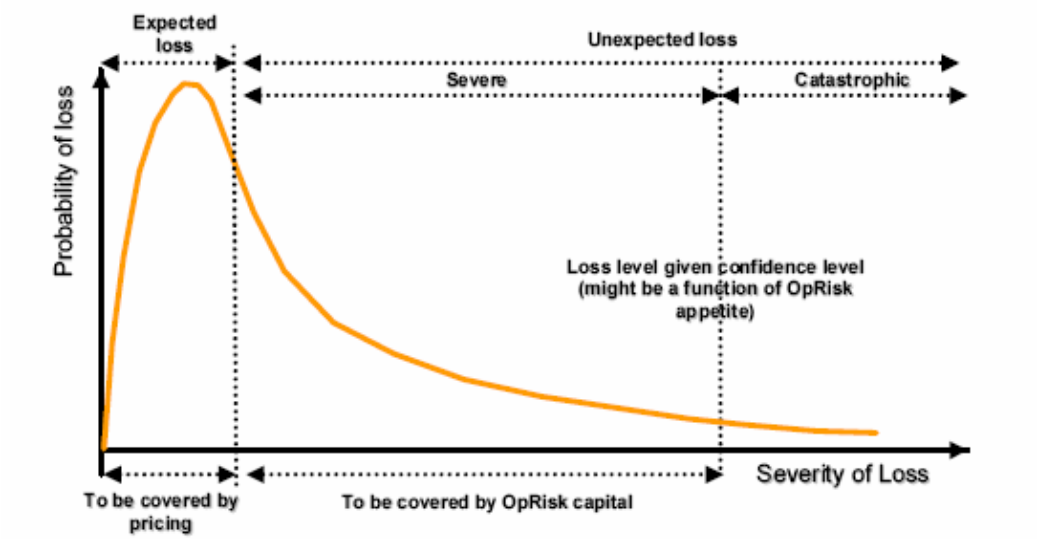

Figure 4. Possible Monte Carlo Simulated Operational Risk Loss

The simulation method offers the following advantages:

- strong quantitative support, once validated with sufficient firm specific data;
- methodology parameters (distribution, confidence interval, holding period) consistent with those employed for market and credit risk;
- a specification which would allow the model to generate operational risk or VaR measures;
- a high degree of integration in the overall risk framework allowing to derive bottom-up capital allocation mechanisms for operational risk.

However, the simulation method has also the drawback of a high degree of complexity, assumptional intransparency and its implementation will require important resources. Also, the present state of data has to wait several years before backtesting or validation is possible.

c) *The scenario models,* which range from quantitative sensitivity analysis to - in their simplest form - qualitative assessments.

These models produce a subjective loss estimate for a given time horizon (one year) and confidence level (99%), based on the experience and expertise of key managers. Weaker assessment forms could just require ranking of the operational risk level for each elements of a risk map or checklist.

Qualitative assessment models have been put forward, as they are particularly well suited for tackling both the frequent inobservability of operational risk and its high context dependency. A purely qualitative assessment can also be turned into a quantification method. This could involve four core elements:

- a check list for a periodic and systematic qualitative assessment of each element of operational risk;
- a grading scale-based assessment considering criteria such as severity, probability and time horizon of occurrence;
- grading dependent management escalation procedures, action triggers, or compensation rules;

- a transformation of the grading into an operational risk level expressed in currency.

Such methods have the advantage of enhancing transparency of the change of operational risk. They also allow a proactive management of the level of operational risk. However, as they rely on the subjective judgement of experts, they are only appropriate for a crude quantification of the operational risk economic capital level and operational risk capital allocation.

It should be underlined that the trend is not to use particular models and techniques on a standalone basis but increasingly in combination with each other to do justice to the complexity of operational risk. This trend of combining various quantification approaches allows firms to make quantification approaches to their own specific operational risk environment.

3. Trends regarding the operational risk in the financial sector

Over the last 10 years, risk management especially for market and credit risks, has reached the impact stage. Operational risk management today is gaining prominence, but the stage of the full quantitative impact has not been reached. Its quantitative foundation - with credible, relevant and meaningful total figures - cannot be expected in the near future.

More and more the followings will become a prevalent development:

- generally increased risk awareness, including operational risk;
- more rational, more analytical attempts to identify, define, categorize, measure, quantify and partly transfer losses and risks;
- closer attention by regulators;
- attention by and responsibility of senior management and Board of Directors;
- operational risk seen in a broader context;
- a fast changing environment, in which operational risk management takes place: boundaries increasingly blur, consolidation and convergence in the industry continue, dis-intermediation and global capital markets grow faster.

The operational risk management of the future has to be seen in the wider context of globalization and Internet-related technologies. The two major future drivers - globalization and Internet-related technologies - will challenge the banks to take on additional and partly new operational risk.

The increasing globality of financial services increases the demands on governance, including environmental and social responsibility.

Globalization with its many advantages for the stakeholders of a modern firm usually adds complexity and diversity of cultures, management and staff. A common culture - and a common risk culture - will be one of the challenges for a globally oriented organization.

Managing a modern company means managing on behalf of all core stakeholders. Creating value for clients, staff and business partners is a precondition for creating shareholder value. Sustained and sound profitability is also the best contribution for avoiding systemic risks and protecting savers.

Ubiquitous computing and Internet-related technologies (IT) make every business a data-based business in a new e-economy, especially in financial services. IT changes everything and it is no longer just a strategy supporter, but a strategy enabler: it enables transactions and services any time, instantaneously, with no barriers, at decreasing prices.

Such a "technical environment" represents a major new challenge for management and especially for Operational risk management. While computing solves many Operational risk problems, it also creates new ones: IT, control, compliance, security, privacy protection etc.

Financial institutions face continued dilemmas which have operational risk ramifications:

- the most venerable versus the most vulnerable;
- innovation "entrepreneurship" and "intrapreneurship" versus structure and processes;
- consistency and predictability versus change and innovation;
- long term orientation versus short term performance pressure;
- security versus speed;
- scale and standardization versus scope and differentiation;
- local conditions versus global pressures;
- maximizing activities where the outcome is controlled and minimizing exposures;
- operating and capital allocation efficiency versus compliance, control and capital requirements of supervision;
- shareholder pressure versus other stakeholders' expectation.

The winners will be those who understand the forces of change best, implement accordingly and "synchronize" their efforts optimally in turbulent times.

Clear structures and processes with defined allocation of responsibilities are preconditions for a successful operational risk management. The control and compliance environment is increasingly checked by supervisors, who more and more ask for individual responsibility.

4. Conclusions

Good operational risk management - in combination with quality management - is a decisive base for enhancing the reputation of a financial institution. In a major crisis, the impact on market capitalization and reputation can be significant during the first few months. Thereafter, the responsibilities for the disaster and the operational risk management capability to deal with the aftermath become more visible. Thereby, consistent and effective communication as well as honesty shows a fundamental financial value.

Financial institutions and regulators/supervisors should be aware of the cost/benefit relationship of setting in place the quantification of operational risk involving data gathering, models, procedures, systems and staff.

The experience of setting up such systems for the quantification of market risks indicates the cost and inertia involved for changing the system and systems for a relatively little disputed analytical approach. Therefore there is no credible and satisfying overall model applicable to operational risk available for the quantification at present, except for some subcategories which might not be relevant in the overall context.

The financial services industry as a whole - not withstanding the major differences among banks - has made considerable progress over the last years in operational risk areas, such as: definition, aspects of strategy and planning, structure, reporting, tools, capital allocation and risk transfer. But there is still a long way to go to reach an effective, credible and implementable operational risk analytical framework.

Operational risk management is becoming more and more a core competency of risk management and of general management. Developments to be expected in this field are the followings:

- a greater general awareness and institutionalization of risk management, including operational risk;
- a more conscious analytical and multi-disciplined integration of credit, market and operational control functions: internal and external audit, legal and compliance, product control, operations, insurance, finance;
- a better focused business approach: a move from a "defensive" position of operational risk management to an "offensive" position;
- strategic planning is linked with risk management and operational risk;
- relevant internal database systems become more commonly defined, standardized, structured, systematic, comprehensive and consistent as part of a modern risk management framework;
- internal economic risk capital models include operational risk in view of more internal rational capital allocation targets;
- more risk transfer to third parties which are able to analyze, diversify and bear operational risk of banks: insurance for external risks and for integrated risk products as well as for standardized capital market transactions.
- new regulatory and supervisory standards and entities converge, cooperation and information sharing between supervisors gets closer.

Therefore, operational risk management is a continuous learning process: operational risk management is not a program, it is a continuous, diligent process throughout an organization.

REFERENCES

1. Avery, R., Milton, P. "Insurers to the Rescue?", Risk Professional, Special Issue on Operational Risk, Spring 2000, pp.61-69
2. Jameson, R., Operational Risk and Financial Institutions, Risk Books, Arthur Andersen, UK, 1998.
3. Kimball, R. "Failures in Risk Management", New England Economic Review, Jan./Feb. 2000, pp. 3 -12.
4. Morris, S., Operational risk Control, What FSA Expects... and You Must Do, CMS, London, Jun. 2000
5. Pîrvu, C. Mehedințu,A. Buligiu, I. "A model of costs'analysis and prognosis", 6th International Symposium: Economy and Business 2007 - Economic Development and Growth, International Scientific Publications vol.1, published by Science Invest-Bourgas, Bulgaria, pp. 287-296
6. Young, B., Quantification of Operational Risk, Centre for Operational Risk Research & Education, 200