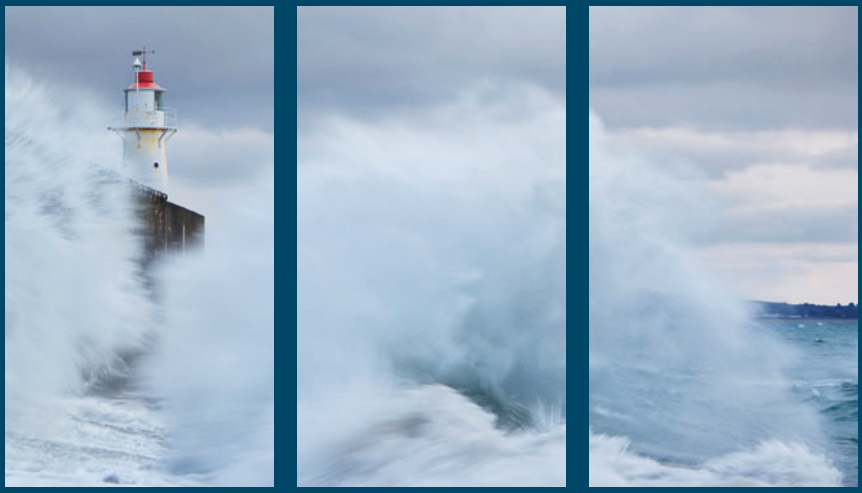
PALGRAVE MACMILLAN STUDIES IN BANKING AND FINANCIAL INSTITUTIONS
SERIES EDITOR: PHILIP MOLYNEUX

Operational Risk Management in Banks

Regulatory, Organisational and Strategic Issues



Giuliana Birindelli
and Paola Ferretti

Palgrave Macmillan Studies in Banking and Financial Institutions

Series editor
Philip Molyneux
Bangor University
Bangor, UK

The Palgrave Macmillan Studies in Banking and Financial Institutions series is international in orientation and includes studies of banking systems in particular countries or regions as well as contemporary themes such as Islamic Banking, Financial Exclusion, Mergers and Acquisitions, Risk Management, and IT in Banking. The books focus on research and practice and include up to date and innovative studies that cover issues which impact banking systems globally.

More information about this series at
http://www.springer.com/series/14678

Giuliana Birindelli · Paola Ferretti

Operational Risk Management in Banks

Regulatory, Organizational and Strategic Issues

palgrave
macmillan

Giuliana Birindelli
Department of Management
and Business Administration
"G. d'Annunzio" University
of Chieti-Pescara
Pescara, Italy

Paola Ferretti
Department of Economics
and Management
University of Pisa
Pisa, Italy

This book is the result of the joint efforts of the two authors, who equally contributed to the work.

Palgrave Macmillan Studies in Banking and Financial Institutions
ISBN 978-1-137-59451-8 ISBN 978-1-137-59452-5 (eBook)
DOI 10.1057/978-1-137-59452-5

Library of Congress Control Number: 2017937472

Cover credit: Helen Dixon/Alamy Stock Photo

Printed on acid-free paper

This Palgrave Macmillan imprint is published by Springer Nature
The registered company is Macmillan Publishers Ltd.
The registered company address is: The Campus, 4 Crinan Street, London, N1 9XW, United Kingdom

To Stefano and Giorgio

Contents

1	**Introduction**	1
2	**The Operational Risk: An Overall Framework**	9
3	**The Regulatory Framework**	37
4	**Operational Risk Management: Organizational and Governance Issues**	67
5	**Operational Risk Mitigation: Strategies and Tools**	111
6	**Operational Risk Modelling: Focus on the Loss Distribution and Scenario-Based Approaches**	133
7	**Operational Risk: Evidence from Italian Cooperative Banks**	169
8	**Disclosure on OR: Evidence from a Sample of Italian Banks**	199
Index		217

List of Figures

Fig. 4.1	Example of information flow between the OR function and internal audit (Garnero 2003)	94
Fig. 4.2	Example of information flow between compliance function and OR function (Birindelli and Ferretti 2013)	96
Fig. 5.1	Insurance impact on the Loss distribution curve (Scott and Jackson 2002)	119
Fig. 6.1	The scenario funnel (OeNB and FMA 2006)	158
Fig. 8.1	The disclosure rating (own processing)	214

List of Tables

Table 2.1	Operational losses: cause categories and activity examples (Prokopenko and Bondarenko 2012)	17
Table 2.2	BCBS: comparison of risk definitions (Birindelli and Ferretti 2013)	31
Table 3.1	Standardized approach: business line, list of activities, percentage (EU-CRR 575/2013)	41
Table 4.1	Tasks of OR functions/officers (Metelli 2005)	85
Table 4.2	OR Governance internal structure (Prokopenko and Bondarenko 2012)	87
Table 5.1	Insurance recoveries (BCBS 2009)	122
Table 5.2	Insurance recoveries by event type (BCBS 2009)	123
Table 7.1	Types of OR approaches by level of diffusion among banks	170
Table 7.2	Size of BCCs participating to the survey—values in thousands of euros (own processing)	171
Table 7.3	Responsibility score attributed to the OR function—BCCs in Tuscany (own processing)	173
Table 7.4	Engagement in OR management—BCCs in Tuscany (own processing)	173
Table 7.5	Engagement in OR management—Federlus BCCs (own processing)	176

Table 7.6 Frequency of use of tools for OR assessment—BCCs in Tuscany (own processing) 178
Table 7.7 Frequency of use of tools for OR assessment—Federlus BCCs (own processing) 180
Table 7.8 Reasons relevant for calculation of economic capital—mean values for BCCs in Tuscany (own processing) 181
Table 8.1 Assignment of the disclosure rating (own processing) 213
Table 8.2 Areas of disclosure: average and maximum value (own processing) 215

1

Introduction

The many transformations in the banking industry in the last decades and the series of banking scandals and collapses have emphasized the relevance of operational risk to the extent that the phenomenon has drawn the attention of banking supervisory authorities, practitioners and scholars. The appearance of operational risk can be linked to several elements of change, such as the growing sizes of institutions and their greater organizational complexity as well as of the emergence of new products and business lines; the technological change and the development of e-commerce and e-banking; the more intensive competition and globalization of the financial market. Finally, not least, the recent international financial crisis certainly represents another source of operational risk: its occurrence evidenced several flaws in the organization as, for example, internal controls that should have prevented failures in lending and securitization were not in place. Loan officers failed to identify healthy borrowing firms, rejecting their legitimate loan applications. At the same time, loan officers failed to detect borrowing firms that were heading towards bankruptcy and approved their illegitimate loan applications. Such occasional miscalculations eventually turned into financial losses for the banks. Additionally, securitizations

G. Birindelli and P. Ferretti, *Operational Risk Management in Banks*,
Palgrave Macmillan Studies in Banking and Financial Institutions,
DOI 10.1057/978-1-137-59452-5_1

contributed to transmit the operational risk from one bank to another, creating a domino effect and a systemic risk. Consequently, the financial crisis further evidenced the importance of banks having an effective operational risk management that could ensure financial stability, at both individual and systemic levels.

The need to strengthen controls over operational risks highlights the initiatives of the Basel Committee on Banking Supervision carried out between 2001 and 2006 (Basel 2), aimed at including operational risk in the international regulatory framework. Such initiatives covered a key role in setting a universal definition of operational risk: until then, operational risk had included any risk that did not fall within the category of market or credit risk, clustering residual and heterogeneous risks. The Basel 2 framework defines it as the risk of loss resulting from inadequate or failed internal processes, people and systems or from external events. This definition includes legal risk, but excludes strategic and reputational risks.

The same sources of operational risk are identified in the current UE prudential regulation (Capital Requirements Regulation—CRR—575/2013 and Capital Requirements Directive—CRD—36/2013). Hence, both provisions (Basel 3 and UE legislation) outline a clear causal definition of operational risk that inevitably involves a strict analysis of the processes, systems, people and external events, which represent the possible sources of operational losses.

Compared to other types of risk, operational risk presents some quite distinctive features. First of all it is generally a one-side risk; it tends not to be correlated with the expected return; it is transversal to the whole banking activity, is not easy to be transferred and/or hedged and is not correlated with the bank's size and/or its volume of business. Moreover, while some losses are clearly the result of operational risk, for others it is less clear whether they should be classified as operational risk or other risk categories, thus raising the problem of boundary operational losses. Accordingly, the prudential regulation provides some details on the matter to prevent overestimates, double counting or improper reductions of capital requirements.

The definition of the boundary between operational risk and other risks (credit and market risks) has been identified by the industry as a

fundamental issue towards the consistent collection and modelling of operational risk loss data. Likewise, the definition of operational risk boundaries that distinguish it from other types of risk such as strategic, reputational and compliance risks help avoid overlaps in risk management caused by similarities among the types of risks.

While the complexity of the definition of operational risk and scope represents a crucial matter and is constantly the object of interest for the financial community, great attention is also given to the calculation of operational risk capital requirements. Particularly, the current regulatory framework (Basel 3 and UE CRR 285/2013) provides multiple methods for calculating operational risk own funds and aims to ensure correspondence between the degree of refinement of the approach to the level of an intermediary's risk exposure, to limit the burden of regulation on smaller banks and to formally acknowledge at supervisory level the improvements adopted by banks in operational risk management practices. To this end, alternative approaches have been set out for calculating operational risk capital requirements, each of which incorporates different levels of risk-sensitivity and requires distinct degrees of sophistication: the basic indicator approach, the standardized approach (and the alternative standardized approach) and the advanced measurement approach.

In a continuously changing context, the implementation of operational risk standards is still being monitored by the supervisory authority. In particular, the Basel Committee has recently provided comprehensive guidance regarding the qualitative requirements that should be observed to achieve more rigorous and comprehensive operational risk management. The Basel Committee has also proposed a review of the operational risk capital framework. In order to address a number of weaknesses of the current framework and at the same time ensure the objective of balancing simplicity, comparability and risk sensitivity, the proposal aims to introduce a revised methodology, the standard methodology approach, which should replace the existing standardized approaches for calculating operational risk capital as well as the advanced approach, thereby simplifying significantly the regulatory framework.

In this evolving scenario, both at regulatory and operating level, the organizational, mitigation and measurement issues are more and more crucial. Banks therefore need to develop, implement and maintain a sound operational risk management framework. This hence requires that banks introduce and foster a strong operational risk management culture throughout the whole organization. Moreover, the implementation of a sound operational risk management entails the need for an in-depth analysis of multiple business processes and sub-processes, phases, and activities. Such need reflects the interdependence between the operational risk exposure and the structure of a bank's governance and organization, which has been observed in several cases of financial collapses where losses mainly associated with internal fraud were specifically connected to supervisory and operational failure on behalf of the board of directors and senior management. On the other hand, the focus on organization arises in response to the need of combining measurement systems with efficient and adequate control units for operational risk management.

In order to achieve a comprehensive approach to operational risk, banks should also have appropriate mitigation and transfer strategies. In reference to this aspect, it is important that banks understand the extent to which risk mitigation instruments (e.g. insurance policies) truly reduce the operational risk exposure, transfer the risk to another business sector of financial system or create new risks. Regulators recognize risk transfer or insurance as a mitigation tool only for the advanced approach and the eligibility of the instruments is subject to specific requirements. Such opportunity has underlined in particular the strategic importance of insurance portfolio management in banks. The development of the use of insurance within the operational risk management may in fact contribute to the reduction of the capital charge and the economic impact linked to the operational losses. On the other side, there are a number of challenges, such as the difficulty in measuring the extent of insurance's mitigating effect and the need to effectively match insurance products with operational losses (insurance mapping).

Lastly, a sound operational risk framework depends on the adequacy, completeness and accuracy of the data used for building the measurement model. The degree of flexibility that banks have had in operational

risk modelling has fostered the development over the years of a variety of methods. Currently, these may be linked to two categories, namely the loss distribution approach and the scenario-based approach. The former is derived from the actuarial science; it is a rather widespread practice but yet presents some methodological limitations. One, for example, is the assumption that the past is a reliable representation of the future, which may result both in under-representing the events that never occurred in recent memory and for which data is not available, and in over-representing the events that happened very frequently in the past and that have already been mitigated. In order to overcome the methodological limitations of the Loss Distribution Approach (LDA), the best practices tend to combine this approach with the Scenario-Based Approach (SBA), which sums the knowledge of experts who demonstrate a deep understanding of the bank's business, threats and vulnerabilities and who make the operational risk calculation more responsive to the existing business processes and ensure that the bank is attending to its key operational risks. This way qualitative and quantitative approaches are combined to build loss distributions for individual and aggregate operational risk exposure, incorporating experts' opinion of risk correlations and dependencies.

The great complexity connected with a proactive management of the operational risk may represent an obstacle to its development by smaller banks. There is no doubt that in the case of small financial institutions the operational risk takes on a secondary role compared to other risks, more closely associated with typical banking activity (e.g. credit risk). This can be mainly due to the low degree of diversification of the activities carried out by smaller banks, which decreases the operational risk exposure and consequently the need to employ human, financial and technological resources in sophisticated systems of operational risk management. Nevertheless, it is crucial to examine how small-sized banks manage their operational risk exposure in order to understand the most important gaps and shortcomings and hence identify the opportunities of improvement for helping to create a level playing field.

Although there are differences in the operational risk management depending on the size of the bank, it is possible to point out that the operational risk management is still generally at a stage of development,

and calls for a greater commitment and awareness for a proactive management. This may be supported also by the disclosure requirements (Pillar 3). The current regulatory framework requires banks to provide accurate and comprehensive disclosure of their operational risk profile; in particular, banks are asked to disclose the approaches for the assessment of their own funds requirements.

The present book is divided into a total of eight chapters. The following chapter (Chap. 2) "The operational risk: an overall framework" describes the specific features of operational risk, as well as its origin and main sources. It also draws particular attention to the similarities and differences with other risks—credit, market, strategic, reputational and compliance risks.

The third chapter "The regulatory framework" analyses the main features of all the approaches for calculating the capital requirement for operational risk, highlighting critical issues of each approach. Finally, it provides a short description of the most recent initiatives of the Basel Committee; noteworthy is the recent new standardized measurement approach for operational risk proposed by the committee, as part of the broader objective of balancing simplicity, comparability and risk sensitivity.

The fourth chapter "Operational risk management: organizational and governance issues" examines the organizational and governance issues related to the measurement and control of operational risk, focusing on the key functions involved (e.g. committee, operational risk functions), on the interrelationship between the operational risk function and other functions (internal audit and compliance), as well as on the role of reporting and IT.

The fifth chapter "Operational risk mitigation: strategies and tools" provides a description of the regulatory framework of the operational risk mitigation techniques, focusing particularly on insurance, the main operational issues of their use as operational risk mitigants, with an emphasis on the most relevant impacts on the banks' operational risk management. Finally, it reviews the most widespread instruments available to banks, both traditional and innovative ones.

The sixth chapter "Operational risk modelling: focus on the loss distribution and scenario based approaches" aims at analysing the specific

features of both the methodologies, highlighting strengths and weaknesses of each. As it is not possible to state which approach is the best in absolute terms, according to the best practices, the combined use could be the preferable choice.

The seventh chapter "Operational risk: evidence from Italian cooperative banks" reports the results of a survey on a sample of Italian cooperative banks. The survey explores different research areas: organizational aspects, measurement methods, Second Pillar, insurance coverage, and trade associations/outsourcing.

The eighth (and the last) chapter "Disclosure on OR: evidence from a sample of Italian banks" illustrates the degree of disclosure of the operational risk management; in particular, it reports the evidence of a survey on a sample of listed banks in Italy, focused on the following areas of investigation: general aspects, organizational structure, measurement systems, control, mitigation and transfer systems, and capital.

2

The Operational Risk: An Overall Framework

2.1 Introduction

Since the 90s, several factors (e.g., the growing size of the banks, the massive technological investments, the development of e-commerce and e-banking, the outsourcing of production processes) induced to revise operational risk management tools and to reflect on the introduction of specific regulatory requirements. Further attention towards operational risks was brought about by the awareness of the catastrophic nature that operational risk can lead to, in some cases, even compromising the survival of the financial intermediary.

In this chapter we focus on the specific features of the operational risk, as well as its origin and main sources. Particular attention is also given to the similarities and differences with other risks, namely credit, market, strategic, reputational and compliance risk.

G. Birindelli and P. Ferretti, *Operational Risk Management in Banks*,
Palgrave Macmillan Studies in Banking and Financial Institutions,
DOI 10.1057/978-1-137-59452-5_2

2.2 Definition and Classification of Operational Risk

In recent years the supervisory authorities have recognized operational risk (OR) as a relevant phenomenon transversally pervading the entire banking industry. For years the existence of many operational risks (ORs) has often become apparent only after the high losses of many banking crises and has often taken the guise of a different type of risk exposure (e.g., credit or market risk), which was consequently addressed inappropriately, underestimated or not addressed altogether.

Although operational risk is innate to banking itself, over the years the phenomenon has been mitigated by pursuing a typical ex-post approach and has only recently been identified by a formal definition (see below). Starting from the 90s a number of factors induced to revise OR management tools and to reflect on the introduction of specific regulatory requirements. These factors are well-known (Ellis et al. 2012); among these, the most important are as follows:

- the growing size of the banks, accompanied by an increasingly complex organization, by the emergence of new business models (e.g., investment services, multi-channel distribution) and—in the presence of Merger & Acquisition (M&A) operations—by possible distortions in integrating the operational and information systems of the companies involved in the process of aggregation;
- the massive technological investments made by banks, in which various types of OR were concealed (human errors and system faults);
- the development of e-commerce and e-banking, exposed to external frauds, problems of security and cybercrime;
- outsourcing of production processes, which arouses uncertainties in the sharing of responsibilities;
- the widespread use of credit and market risk mitigation instruments, such as derivatives and securitization, followed by the increased presence of specific ORs (Carosio 2001). In this respect, evidence has also resulted from the crisis of the US subprime mortgages: the analysis of 86 cases reported in the FIRST (Facts on International

Relations and Security Trends) database concerning the operational loss events has shown that the underlying causes of many of the events connected with the crisis are inadequate controls, as well as improper management behaviour and dysfunctions in the remuneration systems (Cagan 2008).

Further attention towards OR has derived from the awareness of the catastrophic nature that OR can lead to, eventually compromising the very survival of the financial intermediary. Indeed, in the past decades, operational failures have produced dramatic results, in some cases even leading to collapse (Fontnouvelle et al. 2003; Aparicio and Keskiner 2004; Rachev et al. 2006). In the same period, financial institutions have experienced over 100 operational loss events, each exceeding 100 million dollars (Fontnouvelle et al. 2003). The history of sensational financial failures has unveiled a number of contributing factors: dishonest employee behaviour, improper business practices, malfunctioning in the internal control systems, lack of transparency in carrying out investment services, distorted reward systems, unclear reporting lines. These factors have stressed the need to strengthen controls over OR, especially in the financial area, as well as the need to use indicators for monitoring the trends of risk exposure. Some authors have suggested the usefulness of gathering these indicators (including the number of daily negotiations for each trader and the share of remuneration based on bonus mechanisms) in a scorecard approach for capital allocation for ORs and pricing decisions in financial institutions (Sundmacher and Ford 2004).

One emblematic case of OR dates back to 1995, when the reckless and unauthorized financial activities implemented by the trader Nicholas Leeson led to the collapse of Barings Bank (Queen Elizabeth's personal bank), causing $1.3 billion losses. Following the unauthorized derivative transactions in the Asian markets, started in 1992, the first losses were recorded on a secret account, numbered 88888, until Nickolas Leeson—alias, the "rogue trader" (from the title of his autobiography, see Leeson 1997)—started to gamble on market stability on January 16, 1995. The following day Asia was hit by a violent earthquake that caused the collapse of the market, forcing Leeson into increasingly risky recovery efforts, which made losses soar.

Yet, only a few years from that event, the "lesson" from Barings Bank seemed to have been completely forgotten: in February 2002 the reckless operations in the exchange market conducted by Allfirst (a US subsidiary of the Allied Irish Bank) employee, John Rusnak, were followed by fake hedging contracts to hide losses—estimated at $691 million—proving once again the threat represented by rogue trading.

Again, in January 2008 trader Jerome Kerviel caused a $7.1 billion loss to Société Générale, because of unauthorized European Index Future trades. Kerviel's losses came from bets made on "plain vanilla products", relatively simple futures tied to major European stock indexes. In that same year, trader Evan Brent Dooley of MF Global conducted unauthorized futures transactions resulting in a loss of $141 million.

It is apparent that the financial services industry has a perennially short memory. Indeed, in 2011, shortly after the Société Générale trading scandal, UBS reported a similar scenario. Again, another trader, Kweku Adoboli, escaped the firm's risk management radar, losing $2.3 billion on fraudulent exchange-traded funds (ETFs) transactions. Kweku Adoboli set up a secret account nicknamed "umbrella" to hide losses, which exploded after his ever-bigger trades went sour. He also booked fake trades to offset the risk exposure he had created (Poster and Southworth 2012).

Many other trading scandals had involved well-known financial institutions—even before the collapse of Barings Bank—as a result of serious lapses in operational risk control. Among these, the most worth recalling are as follows:

- the securities fraud by Michael Milken, known as the "junk bond king", brought the Drexel Burnham Lambert into bankruptcy, which was fined $650 million (November 1989);
- the $1.1 billion loss by the Daiwa Bank suffered as a result of unauthorized trading of bonds by one of its US managers, Toshihide Iguchi (September 1995);
- unauthorized trading in the copper market by Yasuo Hamakana, member of a team that controlled 5% of the world's copper trading

(and for this reason called "Mister 5%"), which caused losses for $2.6 billion to the Japanese trading company Sumitomo (June 1996);
- at Griffin Trading company (no longer in existence), Scott Szach, chief financial officer of the company, diverted over $5.6 billion from one of the company's bank accounts in favour of a brokerage account in the 18 months prior to the sale of the company (January 2001);
- the $277 million loss to the National Australia Bank, caused by unauthorized currency options on behalf of two traders: Vince Ficarra and David Bullen (January 2004).

The difficulty to uncover such violations in a timely manner can require a proactive management based on the application of modern basic criminological assumptions, aimed at analysing the multi-causal cause-effect relationship in the underlying risk origination process (Rick and van den Brink 2015). Besides, the history of rogue-trading scandals shows that effective trading surveillance cannot be achieved without sustained, regular dialogue between risk managers, traders and management: the majority of trading debacles were attributable to serious lapses in operational risk control.

Lastly, among the banking scandals we shall also recall the London Interbank Offered Rate (LIBOR) scandals, in which unscrupulous traders and managers from some of the largest banks worldwide (e.g., Barclays, UBS, and Royal Bank of Scotland) deliberately and systematically manipulated borrowing rates. Such conduct—far from being the work of isolated "rogue traders"—had become part of business-as-usual in the international money markets (McConnell 2013). Brokers involved in the LIBOR manipulation scandals covered a key role in illicit activities by assisting banks to manipulate the LIBOR benchmark (McConnell 2014).

Over the years, with the uncovering of the first scandals, OR began to gain increasing attention, triggering a debate around its inclusion in the capital requirements framework (Locatelli 2004). In particular, the issue of operational risk capital requirement was much criticized. Considering that banks typically hold cash funds beyond the required capital to absorb future losses, imposing the capital charge for operational risk could have been counter-productive if this had not been

accompanied by an increased incentive to banks to manage and mitigate operational risk. Moreover, at the time there was no clear evidence that the capital charge, computed under Basel 2, could have provided banks with those incentives necessary to reduce their exposure to operational risk (Belhaj 2010).

Discussions on operational risk management had been formerly raised by the Basel Committee on Banking Supervision (BCBS) in 1998, which led to its inclusion in the international regulatory framework developed between 2001 and 2006. Prior to Basel 2, the term "operational risk" had suffered the lack of a univocal and shared definition, considered (compared to credit and market risks) as an accumulation of residual risks and thus a "cluster" of risks featuring heterogeneity in terms of causing event, severity of loss, likelihood of occurrence and type of impact (effective loss, missed opportunity for gains, write-downs of assets, penalties paid to supervisors, and so on). In fact, BCBS (1998) openly agreed there was no universal definition of operational risk: "At present, there is no agreed upon universal definition of operational risk. Many banks have defined operational risk as any risk not categorised as market or credit risk", while a "positive" definition of the expression that describes what OR *is*, can be found in Basel 2 (BCBS 2004) and, originally, in the documents of the Basel Committee of 2001 (BCBS 2001a, b). As stated: "Operational risk is defined as the risk of loss resulting from inadequate or failed internal processes, people and systems or from external events. This definition includes legal risk, but excludes strategic and reputational risk".

Similarly, the same factors responsible for OR are identified in the Capital Requirements Regulation, CRR (Regulation (EU) No 575/2013). Point (52) of Article 4(1) of CRR—mentioned in point (48) of Article 3(1) of the Capital Requirements Directive, CRD (Directive 2013/36/EU) defines "operational risk" as the risk of loss resulting from inadequate or failed internal processes, people and systems or from external events, and includes legal risk. Differently from BCBS (2004), the scope of OR oversees strategic and reputational risks; however, in spite of such differences in the texts, the definition of operational risk within the CRD/CRR must be read consistently with

that of the Basel Accord: reputational and strategic risks should be excluded from the scope of operational risk (CEBS 2010). Moreover, the definition within the CRD/CRR addresses legal risk, model risk and financial transactions for AMA (Advanced Measurement Approaches) institutions (EBA 2015). Model risk is the risk resulting from improper definition of models used for decision-making, errors in the implementation of these models, their use for purposes beyond those for which they were designed, or inappropriate ongoing monitoring of their performance to verify that they remain suitable for their purposes (EBA 2015, Article 5). Financial transactions and legal risk will be discussed in Sects. 2.3.2 and 2.3.5, respectively.

The causal definition of OR involves a careful analysis of the processes, systems, people and external events (Sironi 2003; Brighi 2003), which are the causes from which an OR loss may arise.

In detail, the factors related to processes include events concerning transaction risk (accounting errors, recording errors, and errors linked to the documentation of transactions), security risk (violation of information security due to a poor system of internal controls) and settlement errors (errors in the regulation of transactions linked to securities and currencies with resident and non-resident counterparties). Additional elements include insufficient formalization of internal procedures and errors in the definition and allocation of roles and responsibilities.

Instead, the factors related to systems include malfunctions and errors in the information system, programming errors in the applications, interruptions and corruptions in the network structure, and failure in telecommunication systems. M&A operations and outsourcing of the data processing activity typically cause this type of risk.

As for factors relating to people (Capgemini 2013), we can certainly include errors due to incompetence, negligence or lack of experience, mobbing, fraud, collusion and other criminal activities, violation of laws, regulations, codes of conduct and ethical standards.

Finally, the external events can be traced back to failures or criminal activities of external subjects (thefts, acts of terrorism and vandalism), to political and military events and to natural disasters (earthquakes, fires, floods and so on).

Alongside the above-mentioned definitions of causes/factors, the CRR also provides a classification of events responsible for the losses, leading to seven classes of event types. In particular, this classification of loss event types takes the following categories into account (Article 324):

1. Internal Fraud: losses due to acts aimed to defraud, misappropriate property or circumvent regulations, the law or company policy, excluding diversity/discrimination events, which involve at least one internal party;
2. External Fraud: losses due to acts intended to defraud, misappropriate property or circumvent the law, by a third party;
3. Employment Practices and Workplace Safety: losses arising from acts inconsistent with employment, health or safety laws or agreements, or from payment of personal injury claims, or from diversity/discrimination events;
4. Clients, Products and Business Practices: losses arising from an unintentional or negligent failure to meet a professional obligation towards specific clients (including fiduciary and suitability requirements), or from the nature or design of a product;
5. Damage to Physical Assets: losses arising from loss or damage to physical assets from natural disaster or other events;
6. Business Disruption and System Failures: losses arising from disruption of business or system failures;
7. Execution, Delivery and Process Management: losses from failed transaction processing or process management, from relations with trade counterparties and vendors.

Examples of operational losses for each category of loss event type are listed in Table 2.1 (Prokopenko and Bondarenko 2012).

The frequency and severity of ORs and their classification into categories have received much attention throughout a number of studies. In particular, a study conducted by the Institute of Operational Risk ranked the top seven ORs for 2013 (Institute of Operational Risk 2013). Namely, the top ORs identified are as follows:

Table 2.1 Operational losses: cause categories and activity examples (Prokopenko and Bondarenko 2012)

Internal fraud	• Unauthorized activity (transactions intentionally not reported; transaction type unauthorized without monetary loss), intentional mismarking of position • Theft and fraud (credit fraud/worthless deposits; extortion/robbery/embezzlement; misappropriation/malicious destruction of assets; forgery, check kiting, account take-over; tax non-compliance/evasion; bribes/kickbacks insider trading—not on firm's account)
External fraud	• Theft and fraud (theft, robbery, forgery, check kiting) • Systems security (hacking damage, theft of information without monetary loss)
Employment practices and workplace safety	• Employee relations (compensation, benefit, termination issues; organized labour activity) • Safe environment (general liability; employee health and safety rules events) • Diversity and discrimination (all discrimination types)
Clients, products and business practices	• Suitability, disclosure and fiduciary (fiduciary breaches/guideline violations; suitability/disclosure (know your customer and know your customer's customers); retail customer disclosure violations, breach of privacy, aggressive sales; account churning, misuse of confidential information) • Improper business/market practices (antitrust; improper trade/market practices) • Product flaws (product defects; model errors) • Selection, sponsorship and exposure (failure to investigate client; exceeding client exposure limits) • Advisory activities (disputes over their performance)
Damage to physical assets	• Disasters and other events (natural disaster losses; human losses from external sources—terrorism, vandalism)
Business disruption and system failures	• Hardware; software • Telecommunications; utility outage/disruptions

(continued)

Table 2.1 (continued)

Execution, delivery and process management	• Transaction capture, execution and maintenance (miscommunication, data entry/maintenance/loading error; misused deadline/responsibility; model/system mis-operation; accounting/entity attribution error; other task mis-performance; delivery failure; collateral management failure; reference data maintenance) • Monitoring and reporting (failed mandatory reporting obligation; inaccurate external report) • Customer intake and documentation (client permissions/disclaimers missing; legal documentation missing/incomplete) • Client account management (unapproved access provided to accounts; incorrect client records (loss incurred); negligent loss or damage of client assets) • Trade counterparties (non-client counterparty mis-performance; non-client counterparty disputes) • Vendors and suppliers (outsourcing; vendor disputes)

1. Regulatory Change: arises from the split of the Financial Services Authority into different entities (the Financial Policy Committee, the Prudential Regulation Authority and the Financial Conduct Authority), an event which increased issues and concerns of many risk professionals about the exact perimeter of authority and what lies within the province of each of these entities. This in turn may increase risks of non-compliance for supervised entities.
2. Systemic Operational Risk: includes operational events affecting a large number of institutions. Examples are the LIBOR scandals, payment protection insurance mis-selling and large IT breakdowns.
3. Internal Model Complexity: a relevant risk in the financial sector, which still requires future effort in order to combine simplicity and reliability in modelling risk.

4. Incentives Misalignment: staff compensation management may have devastating effects if this is not aligned to risk management imperatives.
5. Change: shifts in strategies, policies and conducts may draw the attention away from risks, that therefore may remain unnoticed in the noise of novelty.
6. IT and Data Integrity: IT security and data protection have become significant in the last few years, especially owing to the widespread use of smart phones and social media.
7. Cost Pressure: the financial crisis and its related economic turmoil have resulted in a reduction in staff and systems. These cuts, in turn, overworked employees and systems, thus increasing risk factors.

The financial crisis started during 2007–2008 has highlighted several aspects of operational risk management. Firstly, although the crisis has caused its most significant impact along one business line (namely, trading and sales), it has affected the retail brokerage as well (Hess 2011). This was confirmed by Cope and Carrivick (2013), who further underlined that the impact of the crisis was circumscribed to only a few lines of business, loss categories and types of banks, in terms of both loss frequency and severity. Secondly, the banks' largest losses have not been firm-specific, but have involved multiple banks, since the same types of misconduct are being fined at the same time by multiple regulators, giving origin to what was later coined as "systemic operational risk events": operational risk events that affect the industry as a whole (McConnell and Blacker 2013; McConnell 2015). Finally, operational risks have shown to be related to the typical lending policies of banks. Loan officers have failed to distinguish healthy borrowing firms and have rejected their legitimate loan applications. Furthermore, loan officers have failed to identify borrowing firms that eventually would have gone bankrupt and wrongly approved their illegitimate loan applications. These occasional miscalculations obviously have transformed into financial losses to the lending institutions (Parnes 2012).

Compared to other types of risk (see the sections below), OR presents several clear distinctive elements. These include the following:

- the nature of OR as pure risk or "one-side risk", with the exception of a few isolated cases of income opportunities (deriving, for example, from changes in the regulatory and fiscal environment);
- the lack of a correlation between risk and expected return for OR, except for some sporadic cases like the one in which a greater risk is associated with cost savings in terms of lower investments in procedures and in internal controls;
- its presence across production and support activities, originating the need to create awareness and training across multiple business lines: many operational risks are not localized in defined processes, activities and products, but are transversal to many activities carried out by financial institutions and can concern all the products offered (fraud, aggressive sale, and so on);
- the difficulties in pricing and the transfer/hedging actions;
- no clear correlation between OR, on the one hand, and size of the company and the volume of transactions on the other;
- the interdisciplinary approach required for OR modelling, involving multiple key functions (i.e., Internal Audit, Risk Management, Organization, Accounting, Planning and Management Control, Information Technology). In fact, market and credit risk are managed where they originated (market risk in the Treasury or in the Finance Department, the credit risk in the Credit Department), whereas the OR is run by many functions. Hence, in order to prevent the same problem from being addressed in different ways or with inconsistent timing for the different functions involved, it is necessary to establish a strong coordination among the different structures and a prompt sharing of the information available;
- calculation procedures of the capital at risk. The capital requirements for OR, calculated on a consolidated basis and allocated to companies, do not derive from the sum of capitals calculated at an individual level. This implies the need to define adequate allocation mechanisms that are shared by the companies, reflecting the risk exposure of these companies, and enabling and encouraging an active management of the operational risks so as to reduce risk exposure.

2.3 Main Similarities and Differences Between OR and Other Risk Categories

One of the main features of operational risk is represented by the presence of OR causal factors "behind" many of the losses that might be assigned to other types of risk, thus raising the problem of boundary operational losses. Accordingly, the prudential regulation provides some details on the matter to prevent overestimates, double counting or improper reductions of capital requirements. The definition of the boundary between operational risk and other risks has been identified by the industry as a fundamental issue in the consistent collection and modelling of operational risk loss data. The sections below will treat the similarities and differences between OR and credit risk, market risk, strategic risk, reputational risk and compliance risk.

2.3.1 Operational Risk Versus Credit Risk

By the term "cross-credit" cases we refer to those events that have an operational cause but feature an economic impact that is stored in the database for the capital requirements for credit risk. Likewise, by the term "credit risk boundary losses" we refer to the losses on loans originated by OR events, such as the losses deriving from errors or frauds in the process of credit granting and management.

The wealth of information collected on "cross-credit" cases makes it difficult to define an adequate flow of information, and requires the involvement of (i) the structures responsible for monitoring the exposure to credit risk and its quantification, and (ii) the structures responsible for controlling and managing the operational risks, so that the parties involved can analyse the risky situations, and define any necessary mitigation actions. It also requires the identification of the most appropriate structures for reporting significant events, the clear allocation of responsibilities, as well as the definition of the timing and reporting procedures. Accordingly, the best solution may be to involve the centralized structure rather than the decentralized ones, consistently

with powers held to the former in the control over credit risk exposure and in the recovery of problematic exposures.

The following are some non-exhaustive examples of cross-cases between operational risk and credit risk (Bazzarello and De Mori 2009):

- Internal Fraud: voluntary alteration of the data presented towards the assessment of creditworthiness (for example, changing the parameters used for evaluation, such as personal data or estimates of the guarantees, and lack of consideration of prejudicial events related to the applicant for credit); fraudulently granting loans to fictitious customers; wrongful acquisition/redemption of guarantees; identity fraud;
- External Fraud: presentation of false personal data or of false data relative to one's financial condition upon credit application; falsification of external appraiser valuations regarding the guarantees; presentation of bills/invoices for collection concerning fictitious or already extinct credits;
- Clients, Products and Business Practices: involuntary or negligent management of the credit lines in a manner which is non-compliant with internal rules and/or relevant regulations;
- Execution, Delivery and Process Management: failure to recover the credit due to the loss of supporting acts/documents; delay in the execution of credit recovery processes; negligence in assessing customer creditworthiness; negligence in monitoring the credit exposures of the bank and the connected recovery actions; incomplete or incorrect management of contract updating; negligence in the acquisition, management and conservation of guarantees (e.g., weaknesses in the management of guarantees due to errors in the preparation of the relevant documentation: invalid clauses, ambiguous terms, and so on).

Currently, for AMA institutions, the operational risk losses that are related to credit risk and that the institutions have historically included in the internal credit risk databases must be recorded in the operational risk databases and identified separately. Such losses are not subject to operational risk charge, provided that the institutions continue to treat them as credit risk for the purpose of calculating their own funds

requirements (CRR, point (b) of Article 322(3), see Chap. 3). In particular, EBA (2015) makes specific reference to two operational risk losses related to credit risk: "first-party" and "third-party" fraud (Article 30(1)). The first-party fraud occurs at the initial stage of the lifecycle of a credit relationship in relation to a credit product or credit process and is committed by a client using its own personal account (e.g., inducement to lending decisions based on counterfeit documents or misstated financial statements, such as non-existence or over-estimation of collaterals and counterfeit salary confirmation). Instead, third-party fraud, which always occurs in a credit product or credit process, is committed by a third party who acts illicitly using the credentials of another (unaware) person (e.g., electronic identity fraud—phishing—and use of clients' data or of fictitious identities in the case of loan applications; fraudulent third-party use of clients' credit cards).

2.3.2 Operational Risk Versus Market Risk

By the term "cross-market" cases, we refer to cases that are generated by operational events (e.g., purchase/sale of the wrong amount of financial instruments), but which are uncovered by the controls on market risk. Some non-exhaustive examples of cross-cases between operational risk and market risk are as follows:

- Internal Fraud: voluntary closing of operations by traders at non-market prices/parameters;
- Business Disruption and System Failures: partial or total unavailability of market access systems, preventing the execution or correct performance of operations;
- Execution, Delivery and Process Management: errors during the execution of the orders (e.g., purchase/sale of the wrong security; execution of purchase rather than sales orders, and vice versa; processing of orders with errors in the amount of financial instruments or currency by which they are expressed); closing positions due to errors in the evaluation process (failure to update the price or other relevant parameters).

In 2010 CEBS dealt with the issue "Operational risk versus market risk", defining some criteria of discrimination between the two risks (CEBS 2010). Accordingly, the scope of OR should include:

- Events due to operational errors (e.g., errors in the input or execution of orders, errors in classification due to the software used by the front and middle office, technical unavailability of access to the market).
- Events caused by failures in the internal control system (failures in properly operating a stop loss, unauthorized positions exceeding the allocated limits, and so on).
- Events depending on an incorrect selection of the models outside well-defined processes and formalized procedures (e.g., selection of a model without verifying its suitability for the financial instrument to be evaluated and for the current market conditions).
- Events resulting from incorrect implementation of the models (e.g., errors in in-house IT implementation of a selected model).

In all the above-mentioned cases, the loss should be included within the "scope of operational risk loss", unless the position is intentionally kept open once the OR event is recognized. In this latter case, any portion of the loss due to adverse market conditions occurring after the decision of keeping the position open should be ascribed to market risk.

Conversely, the scope of OR should exclude those events caused by the incorrect choice of a model, if such choice is made through a formalized corporate process in which the pros and cons of the model are carefully examined.

For AMA institutions in particular, EBA (2015) disciplines the "Operational risk events related to financial transactions including those related to market risk" (Article 6). The types of risks reported in the CEBS (2010), as listed above, basically follow the dispositions contained in Article 6 of EBA where, however, the model risk is not mentioned. The model risk is instead disciplined by Article 5 of EBA (2015): "Operational risk events related to model risk". This article also mentions regulatory approved internal models: events related to the under-estimation of capital requirements by these models are excluded from the "scope of operational risk".

AMA institutions are also required to include operational risk losses that are related to market risks within the scope of the own funds requirement for operational risk (CRR, point (b) of Article 322(3); see Chap. 3).

2.3.3 Operational Risk Versus Strategic Risk

In order to avoid misalignment in the banking system and penalties arising from differences in the calculation of capital requirements for OR among financial institutions, there must also be a clear and shared definition of the events and the impacts that need to be handled as operational risks and those to be handled as strategic risks. Moreover, a thorough comprehension of the differences between strategic and operational risk management is key to allow employees within an organization to address risk issues and safeguard organizations from damage.

The current approach tends to consider as losses from operational risk those losses generated by legal settlements or by a voluntary decision on behalf of an institution wanting to prevent any future legal risk. The scope of operational risk also includes events deriving from internal inadequacies, errors and external events that occur when a project is undertaken. On the other hand, losses due to strategic risks are those resulting from incorrect or inappropriate strategic decisions not involving breach in rules, regulations or ethical conduct, and which are not triggered by legal risk (CEBS 2010).

As described by the CEBS, the scope of operational risk extends to the following non-exhaustive examples (CEBS 2010):

- Aggressive selling, resulting from individual initiatives or from the company's need to reach specific objectives, with consequential breaching of regulations, internal rules or ethical conduct;
- Interpretations of the regulations that are contrary to industry practice;
- Refunds to customers as a consequence of operational risk events, before the customers make a complaint but, for example, after the institution has already been required to refund other customers for the same event;

- Tax-related failures resulting in a loss (e.g., penalties, interests on arrears).

In contrast, the following are beyond the scope of operational risk:

- Incorrect decisions of M&A and of organizational-management review;
- Decisions incompatible with the level of tolerance to risk established by the company, when these decisions do not breach rules, regulations or ethical conduct;
- Refunds to customers by the company's own initiative, where no breach of rules, regulations or ethical conduct has occurred.

Furthermore, because some strategic issues may affect an organization as a whole—rather than one or more of its parts—and increase the institution's risk exposure, strategic risks are managed at board level, whereas operational risk affects the day-to-day running of operations and therefore is managed mainly at risk management level.

2.3.4 Operational Risk Versus Reputational Risk

Unlike the above-mentioned cases, for which the supervisory authorities have provided documentation and descriptions, there are no official references for OR in relation to reputational risk. The connections between the two types of risk are, however, numerous.

Indeed, operational events primarily linked to the customer relationships and to breaches in regulation in many cases involve a reputational damage for the bank, especially if it receives significant relevance by the media. For example, the unavailability of IT systems can generate relevant reputational damage also in the case of negligible operational events. Consider for example the case of a malfunction impeding some clients to perform online trading and the consequent amplified diffusion of the piece of news across the media triggered by complaints by the customers involved. The bank's reputation is irreparably damaged.

There are some OR types that occur frequently but have a low impact, and which could be largely underestimated during the

development of mitigation strategies if they were to be considered apart from their reputational component. The case of Automated Teller Machine (ATM) is a suiting example: although the frequent malfunctions may not involve significant operating losses, these events may greatly affect the bank's ability to develop new business opportunities with its own customers or attract new ones. Another example is the diffusion among banks' customers of remote interaction which has offered the banking industry a great opportunity for developing new commercial channels. Despite its potential, this tool entails the risk of betraying the clients' trust if their information is not properly safeguarded: in fact, nowadays the IT Risk Manager's task is not limited to monitoring the risk associated with the availability of data, but extends to issues of integrity and confidentiality of the data, closely related to cyber risk.

Therefore, OR and reputational risk may become strongly interrelated. Indeed, several cases of reputational damage that have occurred in the financial system evidence how OR can trigger the reputational event. This was the case with the scandal mentioned above, involving Société Générale in 2008: in addition to the loss of $7.1 billion and the decline of the security on the stock exchange, it was further hit by the diffusion of the news across the media. Similarly, in 2004 LTSB was fined for having inappropriately sold financial products to its retail clients, thus undergoing significant damage to its image (Bazzarello and De Mori 2009).

Hence, integrating operational risk exposure assessments with quantitative and qualitative assessments for reputational risk is pivotal. It is also important that the possible quantification of reputational risk avoids the double inclusion of losses in the calculation of total capital requirements of the financial institution.

In consideration of these interrelations, it would also be advisable for banks to adopt risk mitigation strategies aimed at containing exposure to both operational and reputational risks. Such strategies should consider multiple approaches, from process revision for improving the internal control system, to investments in information technology, to the implementation of a "risk" and "compliance" awareness culture, and limitation of business activities related to excessively risky products/markets with respect to risk appetite for OR and reputational risk.

Finally, these must be supported by a sound communication strategy, which in some cases can be more effective than risk prevention and management alone. In the event of the bank's risk exposure due to fraud and improper placement of financial instruments to customers, timely communication stating the events occurred and addressing the bank's foreseen plan of action is fundamental in managing the economic impact linked to both the OR and to the reputational effects in terms of lost revenues (Bazzarello and De Mori 2009).

2.3.5 Operational Risk Versus Compliance Risk

As stated in Sect. 2.2, the CRD (Directive 2013/36/EU) explicitly includes legal risk in the definition of operational risk, following the Basel 2 Accord closely. Legal risk embraces all types of events causing losses or other expenses, which are triggered by a breach of rules resulting in legal proceedings or in other voluntary actions on behalf of the institution undertaken to avoid future legal risks. Misconduct events are explicitly included in the list of legal risk cases. EBA (2015), Article 4, provides details on the definition of risk, explaining the meaning of "breach of rules", "rules", "legal proceedings", "other voluntary actions", and "other expenses".

CEBS (2010) interprets the definition of OR contained in the Directive by including in OR any type of legal event triggered by operational risk, regardless of how it is labelled (e.g., compliance risk, environmental risk). Likewise, EBA considers compliance risk as falling within OR. To a certain extent, the definition of legal risk overlaps with that of compliance risk provided by EBA (2011): "Compliance risk (being defined as the current or prospective risk to earnings and capital arising from violations or non-compliance with laws, rules, regulations, agreements, prescribed practices or ethical standards) can lead to fines, damages and/or the voiding of contracts and can diminish an institution's reputation." However, in the Single Rulebook Q&A (Question ID: 2014_1153) EBA addresses the issue of whether the definition of operational risk includes compliance risk, i.e., risk arising from an institution's non-compliance with its legal or statutory responsibilities or

requirements. EBA highlights that this risk must be included in the definition of operational risk found in Article 4(1)(52) of Regulation (EU) No. 575/2013 (CRR): it is one of the many different categories of operational risk. Compliance risk is due to a failure—either conscious or unconscious—to implement the requirements of laws, rules, regulations, agreements, prescribed practices or ethical standards, while its effects may be a regulatory penalty or fine. EBA provides some examples of event classification:

- Internal Fraud: lack of formal rules and/or failure to comply with rules on personal transactions;
- Employment Practices and Workplace Safety: unsuitable policies for variable compensation;
- Clients, Product and Business Processes: lack of formal rules and/or failure to comply with rules governing clients, products or business practices;
- Execution, Delivery and Process Management: non-compliance with regulations and internal rules on Anti-Money Laundering.

However, the Basel Committee draws a distinction between operational risk (BCBS 2004) and compliance risk (BCBS 2005). On the one hand, OR is "the risk of loss resulting from inadequate or failed internal processes, people and systems or from external events. This definition includes legal risk, but excludes strategic and reputational risk". Moreover, legal risk includes, but is not limited to, exposure to fines, penalties, or punitive damages resulting from supervisory actions, as well as private settlements. On the other hand, compliance risk is defined as the risk of legal or regulatory sanctions, material financial loss, or loss to reputation that a bank may suffer as a result of its failure to comply with laws, regulations, rules, related self-regulatory organization standards, and codes of conduct applicable to its banking activities ("compliance laws, rules and standards").

The definitions reported above (BCBS 2004, 2005) present clear differences between the two risks both in terms of the events and consequences, and some triggering events are easily attributed to one type of risk or the other (e.g., damage caused by natural disasters, vandalism,

external frauds and other external events is clearly attributable only to the OR). A further distinction that clearly emerges from a comparison of the definitions is referred to the effects. Unlike compliance risk, quantification of the OR does not need to capture the impact on reputation: indeed, in the definition of OR the exclusion of reputational risk is explicit, while the reference to reputation appears in the definition of compliance risk.

Yet, there are also many convergence points, which might lead to the possibility of considering compliance risk as an OR component (e.g., this is the case of the Unicredit Group; see UniCredit, Reports and Consolidated Balance Sheet 2015), as well as lead to multiple synergies and collaborative relations between the functions governing the two types of risk. This close relationship is also recognized by the Basel Committee (BCBS 2005), according to which there is "a close relationship between compliance risk and certain aspects of operational risk", owing to the existence of a "grey area".

In fact, the existence of cross-cases emerges from a "grey area" that comprises contractual breaches (expressly listed among the events that bring about operational risk) and the bank's responsibility because of non-compliant behaviour, which leads to lawsuits included in legal risk (ABI and DIPO 2009). The inclusion of legal risk in operational risk is the first and foremost cause of uncertainties on the borders and the distinctions between the various forms of risk.

By comparing the causes of compliance and operational risks (Table 2.2), we may evince that the cases of unsuitable rules and internal procedures are common and that there is a greater variety of operational risk events, including the so-called "pure" risk events. There is some uncertainty around the fact that all non-conformities automatically translate into a compliance risk: the range of operational risk instances would be reduced arbitrarily. For example, an internal fraud that had occurred in the presence of inadequate control procedures on the authorization of the operations would be included in compliance risk, despite its being an operational risk. The same reasoning applies to a crash in the information technology system caused by a natural disaster without the restoration of operations, owing to a violation of the business continuity system: this too is an event belonging to operational

risk and not to compliance risk. Besides, intentionality should not be considered a valid discriminating criterion, as wrongful behaviour cannot be assessed differently by simply being justified as deriving from carelessness or forgetfulness, whether wilful or not (Birindelli and Ferretti 2013).

Table 2.2 shows a greater variety of effects for compliance risk: it makes explicit reference to loss of reputation (second pillar risk), while the losses should be material, with the debatable consequence of excluding minor damage depending on normative violations. Compliance risk can affect (or not) reputation, and reputational risk can conceivably occur without generating compliance risk, in accordance with its nature as second level risk: an operational error could also impact the bank's image. However, the exclusion of reputational risk from operational risk, whose events often lead to loss of image, has raised objections in the literature (Lawrence 2003).

Likewise, legal risk, a component of operational risk, does not include effects on reputation. Moreover, its causes differ from those of compliance risk: despite common sources, the violation of self-regulation rules is to be attributed to compliance risk alone. Conversely, the losses deriving from inadequate and incorrect legal documentation

Table 2.2 BCBS: comparison of risk definitions (Birindelli and Ferretti 2013)

	Compliance risk	Operational risk	Legal risk
Causes	Failure to comply with laws, regulations, and self-regulatory standards (e.g., statutes, codes of conduct)	Inadequate or failed internal processes, people, and systems or external events	Failure to comply with laws, regulations, contractual and extra-contractual liability or other disputes
Effects	Legal or regulatory sanctions, material financial loss, or loss to reputation	Loss	Loss
Risks included	Reputational risk	Legal risk	
Risks excluded		Strategic and reputational risk	

or from documentation with excessively onerous clauses for the bank are included in legal risk, just like the losses due to non-compliant behaviours on behalf of the bank's counterparts rather than of the bank itself.

The affinities between Compliance Function and Operational Risk Function spring from the management of shared risks, but also from the fact that they both constitute second level control structures with the task of identifying the risks involved in processes implemented by different functions. A model of virtuous synergies should be created with the aim of achieving a common purpose: cross risk management, facilitated by a mutual exchange and validation of information (Birindelli and Ferretti 2013).

Finally, it is worth noting that the relationship between compliance risk and legal risk has been analysed in terms of the banks operating in a common legal system (Terblanché 2012). Compliance risk should be considered as a component of legal risk and, in turn, also as a component of operational risk in a common law legal system. Terblanché (2012) defines legal risk as a wide concept that includes all aspects of a legal system, while compliance risk is a narrower concept that only includes the codified aspects of a legal system. Therefore, legal risk includes compliance risk, but compliance risk does not include legal risk.

2.4 Conclusions

For a long time, operational risk has been acknowledged only as a technical issue. Unlike to credit and market risks, considered as the main source of anxiety for banks managers, it seemed that scholars were not interested in this topic. It is in the recent years, when Basel Committee on Banking Supervision began to publish on how banks should manage their exposure to operational risk that researchers became interested in. Events such the collapse of Barings in 1995 and other financial scandals (e.g., Daiwa, Enron, Sumitomo, etc.) have highlighted the real danger of operational risk, in terms of direct losses and damage to reputation, and made the banking industry more convinced to deal with it carefully.

Since then, the operational risk has been the subject of several studies. Many analyses have been focused on the operational risk profile of a bank, described by a matrix of business lines and event type, and on the main factors underlying the bank's operational risk exposure. Great attention has also been given to the evolution of the operational risk over time and to its interrelations with other banking risks. All these discussions found common ground in the Basel 2 capital adequacy framework, where, among others, the operational risk was defined for the first time. The definition raises some questions about the necessity of clearly distinguishing the operational risk from other types of risks (credit, market, strategic, reputational and compliance risk), in order to avoid overlaps in their managing.

References

ABI (Associazione Bancaria Italiana) and DIPO (Database Italiano Perdite Operative) (Gruppo interbancario sulla Funzione Compliance dell'ABI e del Comitato Tecnico Criteri dell'Osservatorio DIPO). 2009. Definitions and possible synergies in the field of operational risk and compliance risk. *Bancaria* 65 (12): 81–87.

Aparicio, J., and E. Keskiner. 2004. *A review of operational risk quantitative methodologies within the Basel-II framework*, 1–26. Accenture Technology Labs.

Bazzarello, D., and V. De Mori. 2009. I rischi operativi: casi cross e strutture di limiti. In Birindelli, G., and P. Ferretti (a cura di), *Il Rischio operativo nelle banche italiane. Modelli, gestione e disclosure*. Roma: Bancaria Editrice.

BCBS (Basel Committee on Banking Supervision). 1998. Operational risk management, September.

BCBS (Basel Committee on Banking Supervision). 2001a. Consultative document-operational risk, supporting document to the New Basel Capital Accord, January.

BCBS (Basel Committee on Banking Supervision). 2001b. Working Paper on the regulatory treatment of operational risk, September.

BCBS (Basel Committee on Banking Supervision). 2004. International convergence of capital measurement and capital standards. A revised framework, June (and updated versions).

BCBS (Basel Committee on Banking Supervision). 2005. Compliance and the compliance function in banks, April.

Belhaj, M. 2010. *Capital Requirements for Operational Risk: An Incentive Approach*. Juillet: GREQAM.

Birindelli, G., and P. Ferretti. 2013. Compliance Function in Italian banks: organizational issues. *Journal of Financial Regulation and Compliance* 21 (3): 217–240.

Brighi, P. 2003. Gestione e misurazione del rischio operativo nel Nuovo Accordo di Basilea sul Capitale, *Economia e diritto del terziario* 3.

Cagan, P. 2008. What lies beneath. Operational risk issues underlying the subprime crisis. *The RMA Journal*, 96–100.

Capgemini. 2013. Your people are your biggest asset and your biggest risk.

Carosio, G. 2001. Rischio operativo, strutture organizzative e controlli: il punto di vista della Banca d'Italia, in Locatelli R., Magistretti E., Scalerandi P., Carosio G., Il rischio operativo, Interventi tenuti nell'ambito delle Giornate Romane dell'A.A.S.S.B., Roma, 9 Novembre, quaderno n. 193.

CEBS (Committee of European Banking Supervisors). 2010. Compendium of supplementary guidelines on implementation issues of operational risk, 27 July.

Cope, E.W., and L. Carrivick. 2013. Effects of the financial crisis on banking operational losses. *Journal of Operational Risk* 8 (3): 3–29.

Ellis, B., I. Kristensen, A. Krivkovich, and H. P. Singh. 2012. Driving value from postcrisis operational risk management, McKinsey Working Paper, no. 34.

EBA (European Banking Authority). 2011. Guidelines on internal governance (GL 44), London, 27 September.

EBA (European Banking Authority). 2015. Final draft RTS on AMA assessment for operational risk, 3 June 2015.

Fontnouvelle, P., V. Dejesus-Rueff, J. Jordan, and E. Rosengren. 2003. Using loss data to quantify operational risk, Federal Reserve, April, 1–32.

Hess, C. 2011. The impact of the financial crisis on operational risk in the financial services industry: empirical evidence. *Journal of Operational Risk* 6 (1): 23–35.

Institute of Operational Risk. 2013. Top seven operational risks for 2013, April 14.

Lawrence, D. 2003. Operational risk implications of Basel II/CP3, *Risk Forum*, 19 June, 5–9.

Leeson, N. 1997. Rogue trader, Sphere.

Locatelli, R. 2004. Basilea 2 e rischi operativi: stato dell'arte e prospettive, Convegno CeTIF – Università Cattolica del Sacro Cuore di Milano, Milano, 18 marzo.

McConnell, P. 2013. Systemic operational risk: The LIBOR manipulation scandal. *Journal of Operational Risk* 8 (3): 59–99.

McConnell, P. 2014. LIBOR manipulation: Operational risks resulting from brokers' misbehavior. *Journal of Operational Risk* 9 (1): 77–102.

McConnell, P. 2015. Modeling operational risk capital: The inconvenient truth. *Journal of Operational Risk* 10 (4): 73–111.

McConnell, P., and K. Blacker. 2013. Systemic operational risk: Does it exist and if so, how do we regulate it? *Journal of Operational Risk* 8 (1): 59–99.

Parnes, D. 2012. Modeling operational risk for good and bad bank loans. *Journal of Operational Risk* 7 (4): 43–67.

Poster, A., and E. Southworth. 2012. Lessons not learned: The role of operational risk in rogue trading, Risk Professional, June. http://www.garp.org.

Prokopenko, Y., and D. Bondarenko. 2012. Operational risk management: best practice overview and implementation. In *Risk professional workshop*, Tirana, Albania, September 10–11.

Rachev, S.T., A. Chernobai, and C. Menn. 2006. Empirical examination of operational loss distributions. In *Perspectives on Operations Research*, ed. M. Morlock, C. Schwindt, N. Trautmann, and J. Zimmermann, 379–401. DUV: Essays in Honor of Klaus Neumann.

Rick, S., and G.J. van den Brink. 2015. Mitigating rogue-trading behavior by means of appropriate, effective operational risk management. *Journal of Operational Risk* 10 (3): 1–20.

Sironi, A. 2003. Il rischio operativo: una nuova sfida per le banche italiane, *Economia & Management* 1.

Sundmacher, M., and G. Ford. 2004. Leading indicators for operational risk: case studies in financial services. http://dx.doi.org/10.2139/ssrn.963235.

Terblanché, J.R. 2012. Legal risk and compliance for banks operating in a common law legal system. *Journal of Operational Risk* 7 (2): 67–79.

3

The Regulatory Framework

3.1 Introduction

The current regulatory framework underlines operational risk as a significant risk faced by banks and requires coverage by own funds. It includes provisions for three alternative approaches for calculating operational risk capital requirements, reflecting the broad diversity among European institutions. These approaches are namely the Basic Indicator Approach (BIA), the Standardized Approach (SA) and the Advanced Measurement Approach (AMA), which incorporate different levels of risk sensitivity requiring different degrees of sophistication.

In this chapter we analyse the main features of all these approaches, highlighting their critical issues. Finally, we shortly describe the last proposals of the Basel Committee, which, among others, propose a new standardized measurement approach for operational risk, as part of the broader objective of balancing simplicity, comparability and risk sensitivity.

3.2 From Basel 2 to Basel 3: An Overview

The prudential treatment of the operational risk (OR) was first regulated under Basel 2 (BCBS 2006). Indeed, after a thorough review of

G. Birindelli and P. Ferretti, *Operational Risk Management in Banks*,
Palgrave Macmillan Studies in Banking and Financial Institutions,
DOI 10.1057/978-1-137-59452-5_3

numerous proposals and an international consultation process, Basel 2 finally set the rules both for the determination of OR capital requirements (Pillar 1) and for the supervisory review process and market discipline (Pillar 2 and Pillar 3).

Subsequently, according to an evolutionary logic and in response to the international financial and economic crisis, Basel 3 (BCBS 2011, 2013) introduced important changes to the capital adequacy regulation for banks, though without altering the essence of the prudential treatment of the OR. Similar to the previous regulatory framework, Basel 3 maintained the articulation into three Pillars: minimum capital requirements (Pillar 1), supervisory review process (Pillar 2) and market discipline (Pillar 3). Basel 3 was then implemented across Europe by the Capital Requirements Regulation (CRR—Regulation No 575/2013 of the European Parliament and of the Council of 26 June 2013 on prudential requirements for credit institutions and investment firms) and Capital Requirements Directive IV (CRD IV—Directive 2013/36 of the European Parliament and of the Council of 26 June 2013 on access to the activity of credit institutions and the prudential supervision of credit institutions and investment firms).

The CRR underlines OR as a significant risk faced by financial institutions and requires coverage by own funds. It includes provisions for three alternative approaches for calculating OR capital requirements, reflecting the broad diversity among EU institutions. These approaches are namely the Basic Indicator Approach (BIA), the Standardized Approach (SA), the Advanced Measurement Approach (AMA), which incorporate different levels of risk sensitivity requiring different degrees of sophistication. In general, the CRR encourages institutions to shift towards more risk-sensitive approaches (Recital 52—CRR 575/2013).

The introduction of multiple methods for calculating capital requirements aims to achieve different objectives: (i) ensure correspondence between the degree of refinement of the approach to the level of an intermediary's risk exposure, (ii) limit the burden of regulation on smaller banks and (iii) formally acknowledge at supervisory level the improvements adopted by banks in OR management practices.

The provisions contained in Pillar 1 do not, however, represent a comprehensive solution for OR management, but must be rather considered as integrating provisions in Pillar 2 and 3. With particular reference to

the Internal Capital Adequacy Assessment Process (ICAAP), banks must develop an appropriate governance logic anchored to the enhancement of a proper risk culture (see Sect. 4.2). Specifically, banks must implement a robust process for evaluating and monitoring operational losses linked to credit and financial activities (Krosner 2008), given that their inappropriate management may affect the intermediary's capital adequacy—as has been observed in some of the crisis events. Moreover, when defining an OR strategy, banks should consider also the definition of the OR and the identification of sources of risk; the identification of the risk's profile; the definition of OR appetite by means of measures easily accessible to management; the models and the tools used for the purpose of operational risk management (ORM); the integration of ORM into the wider risk management activity.

3.3 Own Funds Requirements: The Less Sophisticated Approaches

The general principles governing the use of different approaches state that institutions must notify the competent authorities prior to using the (SA) and that those institutions using the SA cannot revert to the use of the (BIA) unless both the following conditions are met (Article 313—CRR 575/2013):

- the institution has demonstrated to the competent authority that the use of a less sophisticated approach is not proposed in order to reduce the institution's OR-related own funds requirements, and that the reversal is necessary on the basis of nature and complexity of the institution and that it would not have a material adverse impact on the solvency of the institution or its ability to manage OR effectively;
- the institution has received the prior permission on behalf of the competent authority.

Finally, a combination of approaches may also be used—provided institutions have obtained permission from the competent authorities.

Under the BIA, the own funds requirement for OR is equal to 15% of the average over 3 years of the relevant indicator (Article 315—CRR 575/2013). Except for few adjustments specifically provided for in the

CRR (Article 316), the relevant indicator is determined as the sum of the interest receivable and similar income, the interest payable and similar charges, the income from shares and other variable/fixed-yield securities, the commissions/fees receivable, the commissions/fees payable, the net profit or net loss on financial operations and other operating income.

Institutions calculate the average over 3 years of the relevant indicator on the basis of the last three twelve-monthly observations at the end of the financial year. However, special cases are foreseen, for example, in the event the audited figures are not available—in which case the institutions are allowed to use business estimates instead. Or again, if an institution has been in operation for less than 3 years, forward-looking business estimates may be used as alternative for calculating the relevant indicator, provided that historical data are used as soon as they become available. Moreover, whenever an institution can prove that the use of a three-year average in the calculation of the relevant indicator would lead to a biased estimate of the OR own funds requirement (either due to a merger, an acquisition or a disposal of entities or activities), it may obtain permission from the competent authority to amend the calculation in a way that would take into account such events. Finally, negative or null relevant indicators are not to be included in the calculation: the average over 3 years is calculated as the sum of positive figures divided by the number of positive figures.

With specific reference to the SA (Article 317—CRR 575/2013), institutions are required to divide their activities into eight business lines (Table 3.1).

Institutions must calculate the own funds requirement for OR as the average over 3 years of the sum of the annual own funds requirements across all business lines. The annual own funds requirement of each business line is equal to the product of the corresponding percentage and the part of the relevant indicator mapped to the respective business line.

In any given year, institutions may offset negative own funds requirements resulting from a negative part of the relevant indicator in any business line unlimitedly with positive own funds requirements in other business lines. However, where the aggregate own funds requirement across all business lines within a given year is negative, institutions must use zero as the input value to the numerator for that year. Institutions must calculate the average over 3 years of the sum of the annual own funds requirement on the basis of the last three twelve-monthly

Table 3.1 Standardized approach: business line, list of activities, percentage (EU-CRR 575/2013)

Business line	Activities	Percentage (%)
Corporate finance	Underwriting of financial instruments or placing of financial instruments on a firm commitment basis; Services related to underwriting; Investment advice; Advice to undertakings on capital structure, industrial strategy and related matters and advice and services relating to the mergers and the purchase of undertakings; Investment research and financial analysis and other forms of general recommendation relating to transactions in financial instruments	18
Trading and sales	Dealing on own account; Money broking; Reception and transmission of orders in relation to one or more financial instruments; Execution of orders on behalf of clients; Placing of financial instruments without a firm commitment basis; Operation of Multilateral Trading Facilities	18
Retail brokerage	Reception and transmission of orders in relation to one or more financial instruments; Execution of orders on behalf of clients; Placing of financial instruments without a firm commitment basis	12
Commercial banking	Acceptance of deposits and other repayable funds; Lending financial leasing; Guarantees and commitments	15
Retail banking	Acceptance of deposits and other repayable funds; Lending financial leasing; Guarantees and commitments	12
Payment and settlement	Money transmission services; Issuing and administering means of payment	18
Agency services	Safekeeping and administration of financial instruments for the account of clients, including custodianship and related services such as cash/collateral management	15
Asset management	Portfolio management; Managing of UCITS; Other forms of asset management	12

observations at the end of the financial year. The particular cases mentioned for the BIA also apply in the case of the SA as well.

Under the SA, institutions are required to develop and document specific policies and criteria for mapping the relevant indicator for current business lines and activities; such policies and criteria must then be reviewed and adjusted as appropriate for new or changing business activities and risks.

The activity of business line mapping must be performed in fulfilment of a number of principles, as follows (Article 318—CRR 575/2013)[1]:

- institutions must map all activities into the business lines in a mutually exclusive and jointly exhaustive manner;
- institutions must allocate any activity that cannot be readily mapped into the business line framework, but that represents an ancillary activity to an activity included in the framework, to the business line it supports. Where more than one business line is supported through the ancillary activity, institutions must use an objective-mapping criterion;
- whenever an activity cannot be mapped into a particular business line, institutions must use the business line yielding the highest percentage. The same business line equally applies to any ancillary activity associated with that activity;
- institutions may use internal pricing methods to allocate the relevant indicator between business lines. Costs generated in one business line which are imputable to a different business line may be reallocated to the business line to which they pertain;
- the mapping of activities into business lines for OR capital purposes must be consistent with the categories institutions use for credit and market risks;
- senior management is responsible for the mapping policy under the control of the management body of the institution;
- institutions must subject the mapping process to business lines to independent review.

The institution intending to adopt the SA must abide to specific criteria that closely related to its organizational structure (Article 320—CRR 575/2013). In particular, it must have in place a well-documented OR assessment and management system, with clear responsibilities assigned

for this system. It must identify its exposures to OR and track relevant OR data, including material loss data. Such system must be subject to regular independent audits carried out by an internal or external party possessing the appropriate knowledge to perform such audits. Moreover, the institution's OR assessment system must be closely integrated into the risk management processes. Its output must be an integral part of the process of monitoring and controlling the institution's OR profile. Lastly, the institution must implement a system of reporting to senior management that provides OR reports to relevant functions within the institution. The bank must have in place procedures for taking appropriate action according to the information within the reports to management.

Finally, in closing the analysis of the standardized method for calculating OR capital requirements we shall highlight that the competent authorities may permit institutions to use an alternative relevant indicator for the business lines of retail banking and commercial banking (Alternative Standardized Approach—ASA). In particular, in the case of the ASA (Article 319—CRR 575/2013) the relevant indicator is a normalized income indicator equal to the nominal amount of loans and advances multiplied by 0.035; the loans and advances consist of the total drawn amounts in the corresponding credit portfolios. For the commercial banking business line, institutions also have to include securities held in the non-trading book in the nominal amount of loans and advances.

In order to be permitted to use the ASA, the institution's retail or commercial banking activities have to account for at least 90% of its income; a significant proportion of the retail or commercial banking activities should comprise loans associated with a high probability of default; the ASA must be able to provide an appropriate basis for calculating the institution's own funds requirement for OR.

3.3.1 The Less Sophisticated Approaches: Some Critical Issues

Of all the approaches available for calculating the capital requirement for OR, the BIA and the SA evidence a contrast between a conceptual simplicity and the subjective capability—of varying intensity depending

on the method considered—of fully grasping the meaning and measurement of OR. Indeed, these approaches represent approximate OR measures, which are unable to fully address the specificities of individual banks, due to their standardized nature.

This is especially true for the BIA; despite it featuring an intrinsic simplicity in calculation and use of easily available data, it does not take into account specific business areas, nor does it support allocation and enhancement policies of capital. The simplistic connotation of BIA evidences the absence of specific recommendations on its adoption, which is however in all cases subject to the general principles of governance and management of OR. Moreover, the simplistic connotation of BIA explains, in general, the better capacity of such approach to adapt to the smaller bank settings with a more modest level of operational diversification and limited complexity of the measurement systems.

The more "convenient" adoption of the BIA should not, however, hamper the development of the OR management process. Indeed, it is desirable that the bank continues to refine its ORM process after the minimum level of compliance has been achieved. This can be realized, for example, through the activation of an OR management system with assignment of roles and responsibilities and the definition of the process for identifying the relevant indicator in accordance with regulations. In other words, the bank should value the full use of the OR framework considered in its complexity. Some actions in this direction are the establishment and/or strengthening of ties across the bank's organizational functions; the conscious assessment of OR exposure, resulting in the identification of inefficiencies in business processes; the promotion of improvements in the functionality of the business and support processes and in the quality of the internal control system.

On the other hand, the approximate results characterizing the SA go in parallel with the need of complying with certain standards, which may cast doubts on the possibility to draw concrete benefits from the application of this approach—unless it is interpreted as an intermediate step for subsequent implementation of the more advanced approach.

The SA does not provide timely information on the causes of OR and inevitably affects the proper development of strategies to contrast OR. Despite the differentiation of risk among the eight lines of business being a positive factor—especially in comparison with the BIA—the

introduction of identical coefficients for all banks no longer allows to grasp the full impact of the losses suffered by each intermediary. Another critical issue might also be the hypothesis of the perfect correlation between the different loss events, based on the assumption of a simultaneous manifestation of operational losses of the various business lines and thus of availability on the bank's behalf of sufficient capital to face these joint events.

As in the case of the BIA, the approximate risk representation is further influenced by an unconvincing correlation between exposure to OR and the relevant indicator, calculated on the basis of the CRR provisions. Questions also arise in consideration of the average value of the relevant indicator to be referred to the last 3 years, especially in cases where the intermediary takes part in extraordinary corporate finance operations, such as Merger and Acquisitions (M&A).

The assumption of the relevant indicator as proxy for the exposure to OR intuitively implies that the latter increases with the former; taking this to an extreme, on the basis of this relationship between the relevant indicator and the OR exposure, a bank with high profitability and with an efficient OR management system is required to set aside a higher amount of capital compared to a competitor bank with lower margins and perhaps with a weaker OR management. Moreover, the dependence of the capital requirement from the relevant indicator does not allow to capture extremes OR events—such as natural disasters or similar rising from external events—typically unrelated to the bank's business volume. A meaningful measure of bank's activity leads to an adequate quantification of regulatory capital exclusively for activities whose exposure to OR are easily measurable and, therefore, for specific event types attributable to certain business lines and with a probability of occurrence that makes possible a prediction of reliable forecasts (this is the case for instance of fraud on credit cards in the retail banking).

The multiplicity of regulatory percentages—a distinctive feature of the SA compared to the BIA—is intended to reflect the different impact of operational losses on the income capacity of the individual lines of business: those with historically low margins are combined to those with higher percentages, in line with the empirical evidence showing that operating losses have the most impact on specific activities such as those relating to the "trading and sales" and "payment and settlement".

The introduction of a variety of percentages implies a general sensitivity of the income capability of the business lines to OR, hypothesizing low margins (related to high impact operational loss) in business lines with high percentages. Therefore, the event that a bank might suffer a severe loss in operational areas associated with limited OR exposure is underestimated; what is more is that the severity of the loss is defined without weighing the intermediary's characteristics in terms of risk management systems and risk mitigation policies.

Finally, the adoption of the SA is not always accompanied by convenience in terms of reduction in capital requirements. The transition from the BIA to the SA does not automatically generate a capital saving, which is determined by the operational characteristics of the bank and, more specifically, by the distribution of the relevant indicator among the different business lines. As to this latter aspect, it may occur that the relevant indicator is mostly derived from the business lines corresponding to a lower regulatory percentage; in such case the banks may have the advantage of adopting the SA, though, this must be evaluated on a case-to-case basis according to the trade-off between lower capital requirement and implementation SA burden. Conversely, if the margin is formed mainly in business lines with high percentages, the intermediary who opts for the SA is subject to a double penalty: a higher absorption of regulatory capital and higher costs of compliance.

Beyond the considerations above, whether the SA adopted represents an intermediate step towards the Advanced Approach or not, it should not be uncoupled from a progressive enhancement of OR management processes. As observed for the BIA, in this specific case the bank must consolidate more than ever the minimum level of compliance, while aiming at the same time to develop the OR framework to its fullest, in the perspective of exploiting the strategic importance of an effective ORM system. This means first of all ensuring that the compliance requirements of the supervisory authority translate into substantial OR management measures. This refers, for example, to the preparation of a structured process of Loss Data Collection (LDC); the classification of the activities into the business lines in fulfilment with the supervisory instructions; the implementation of supporting IT systems; the setting of the self-assessment processes and internal audits to verify at least the

classification of activities and the calculation of the capital requirement; the activation of an adequate management reporting system.

According to an evolutionary logic, the bank must then strengthen the quantitative and qualitative standards upon which the ORM is based through the assessment of OR exposure also embracing scenario analysis, Key Risk Indicators (KRIs) and historical data; the extension of the self-assessment process and internal audit to the LDC; the wider operational use of the measurement system ("use test").

3.4 Own Funds Requirements: The Advanced Approach

In the case of institutions complying with the general risk management standards and meeting specific qualitative and quantitative standards (the former are summarized in Box 3.1), the competent authorities may authorize the adoption of (AMA) based on the institutions' own OR measurement systems.

As for the case of the SA and the foreseen specifications, institutions using the AMA cannot revert to the use of the less sophisticated approaches. Moreover, as established by the CRR in order to avoid a significant drop in capital requirements after the implementation of Basel 2, up until 31 December 2017 institutions are mandated to calculate their requirements in line with a capital floor (currently set at 80% of the capital requirements under Basel 1).

Box 3.1 Qualitative standards for AMA (Article 321—CRR 575/2013)

The qualitative standards a bank must meet to adopt the AMA in conducting its business ("use test") reflect similar requirements to credit risk for the internal ratings based approach. Such standards include the following:

- an internal OR measurement system closely integrated into the institution's day-to-day risk management processes;
- an independent risk management function for OR;
- a regular reporting of OR exposures and loss experience and procedures for taking appropriate corrective action;

- a well-documented risk management system and routine procedures for ensuring compliance, and policies for the handling non-compliance;
- regular review of ORM processes and measurement systems performed by internal or external auditors;
- internal validation processes in respect of an OR measurement system operation in a sound and effective manner;
- transparent and accessible data flow and processes associated with the risk measurement system.

The quantitative standards (Article 322—CRR 575/2013) include requirements relating both to the AMA process and to its four elements: internal data, external data, scenario analysis, and business environment and internal control factors (BEICF).

The quantitative standards related to process include the following:

- calculation of the capital requirement, comprising both expected and unexpected loss, unless the bank can demonstrate that expected loss is adequately captured in its internal business practices;
- the OR measure capturing potentially severe tail events, achieving a soundness standard comparable to a 99.9% confidence interval over a one-year period;
- the OR measurement system comprising specific key elements to meet the soundness standard, among which the use of internal data, external data, scenario analysis and factors reflecting the business environment and internal control systems;
- a well-documented approach for weighting the use of the four elements in the overall risk measurement system;
- a depiction of major risk drivers affecting the shape of the tail of loss estimates;
- recognition of OR loss correlations across individual OR estimates exclusively in the case sound correlation measurement systems are in place, implemented with integrity and informed on the uncertainty surrounding such estimates, and validation of correlation assumptions using appropriate quantitative and qualitative techniques;
- internal consistency and without multiple counting of qualitative assessments or risk mitigants.

In reference to *internal data*, standards expect the bank's internally generated OR measures to: (i) be based on a minimum historical observation period of 5 years (3 years when a bank first moves to the AMA) (ii) be able to map the bank's historical internal loss data into the business lines (Table 3.1) and into specified event-type categories (see Sect. 2.2), and (iii) provide this data to the regulator upon request. A bank must have in place documented, objective criteria for allocating losses to the specified business lines and event types. In exceptional circumstances, a bank may allocate loss events that affect the entire firm to an additional business line "corporate items".

An institution's ORM system must use relevant *external data*, especially when there is reason to believe that the institution is exposed to infrequent, yet potentially severe, losses. To this end, a bank must have in place a systematic process for determining the situations for which external data should be used and the methodologies used to incorporate the data in the measurement system. Requirements must be met also to document the conditions and practices for external data and subject them to periodic independent review.

In addition to the external data, the bank must utilize *scenario analysis* based on expert opinions, to evaluate its exposure to highly severe events. Over time, the institution shall validate and challenge such assessments with comparisons to actual loss experience that can warrant their reliability.

One core element in an institution's risk assessment methodology is its capability of identifying key *business environment and internal control factors* that can change the institution's OR profile. Each factor must be demonstrated to represent a meaningful risk driver based upon both the previous experience and the judgment of experts from the business areas affected; moreover, the bank must demonstrate that risk estimates are sensitive enough to capture any modifications occurring to such factors. In addition to capturing changes in risk due to improvements in risk controls, the risk measurement framework must also be able to identify potential increase in risk entailed by the greater complexity of activities or increased business volume. The bank must document its risk measurement framework and submit it to independent review within the institution and by competent authorities. Over time, the bank has to

validate and reassess the process and the outcomes through comparison to actual internal loss experience and relevant external data.

Lastly, a bank may be permitted to recognize the impact of insurance subject to specified conditions and other risk transfer mechanisms where it is able to demonstrate that a noticeable risk mitigating effect is achieved (Article 323—CRR 575/2013). The capital reduction arising from the recognition of insurance and other risk transfer mechanisms must not exceed 20% of the capital requirement before the recognition of risk mitigation techniques (for further information see Chap. 5).

3.4.1 Regulatory Technical Standards on AMA

The framework on AMA requirements established by the CRR 575/2013 is completed by Regulatory Technical Standards (RTS) developed by the EBA in accordance with the mandate contained in CRR Article 312. In particular, the CRR mandates the EBA to prepare draft RTS concerning both the conditions for assessing the materiality of extensions and changes to the AMA, as well as to the Internal Rating Based Systems for credit risk (Box 3.2) and the assessment methodology under which the competent authorities permit institutions to use AMA.

Box 3.2 Conditions for assessing the materiality of extensions and changes

In December 2013 the EBA prepared specific RTS, adopted by the European Commission on 12 March, 2014. The key features of these RTS are as follows (EBA 2013):

- the introduction of three categories of model extensions and changes: (1) those requiring permission from the competent authorities; (2) those of a lesser materiality, but still featuring a degree of materiality that requires notification to the competent authorities before their implementation; (3) finally, those of an even lesser degree of materiality, which therefore need only to be notified to the competent authorities in regular intervals, after their implementation;
- the introduction of an exhaustive list of qualitative conditions and the design of the quantitative threshold as back-stop regime. In particular, the extensions and changes falling under a category of lesser

materiality may still alter the own funds requirements. Hence quantitative thresholds are applied as a back-stop measure in addition to qualitative conditions when determining the materiality of an extension and change. The thresholds are based on the percentage change of own funds requirements or, where applicable, of risk-weighted exposure amounts before and after the planned extension and change;
- the inclusion of standardized documentation requirements, which enable competent authorities to assess compliance of institutions with the abovementioned rules.

With regard to the mandate of "assessment methodology under which the competent authorities permit institutions to use AMA", the EBA published specific RTS (EBA 2015) which detail the criteria that competent authorities need to take into account before granting institutions the permission to use the AMA for calculating OR capital requirements.

Such RTS are part of the overall review of internal models undertaken by the EBA and are part of the efforts to harmonize practices for the approval of internal models in the area of OR (and also credit and market risks) models across the EU banking sector. To this end, these RTS set out common standards for the supervisory assessment of an institution's classification, identification, collection and treatment of OR events for management and measurement purposes. The final goal is to ensure that the ORM system is based on a well-founded methodology, is effective in capturing the institutions' actual and potential ORs, is reliable and robust in generating AMA regulatory capital requirements, and is comparable across institutions.

The main features of such RTS are reported in Box 3.3 (EBA 2015), while the major hallmarks of the AMA framework are covered in the following pages.

Box 3.3 RTS—Key features

(1) Under the AMA, an institution uses its own internal model to calculate capital requirements with respect to its OR profile. The elements used to determine the OR profile comprise OR data gathered internally and OR data taken from external sources. The regulation (neither the CRD 36/2013 nor the CRR 575/2013) does not provide indications of the scope of OR, leaving the definitions open to different interpretations and allowing institutions to choose how they are implemented; this can

have effects in relation to OR regulatory capital and management practices as well as with regard to supervisory assessment purposes. Indeed, institutions with similar events and losses in OR may come up with significant differences in terms of OR profile and AMA regulatory capital.

(2) With the intention of ensuring uniform application of the scope of OR across the EU, and avoiding inconsistencies in the determination of institutions' OR profile, the RTS set out common standards for the supervisory assessment of an institution's classification, identification, collection and treatment of OR events and losses for management and measurement purposes. Authorities must refer to these criteria when assessing whether an institution AMA framework is effective in capturing and representing its OR profile.

(3) Sound ORM represents, among others, the foundation of an effective ORM framework. To this end, the RTS also introduce common standards for the supervisory assessment of the qualitative elements of an AMA framework; particular focus is given to the role and responsibilities of the OR management function, the "use test" requirement, the data quality and IT systems and the scope of audit and validation functions.

(4) OR modelling is a relatively new and evolving discipline, and each institution has a certain degree of flexibility in building its OR measurement system. However, this flexibility should not favour the development and implementation of ineffective, inconsistent, or insufficiently risk-sensitive internal risk models. For example, the CRR 575/2013 requires an institution adopting the AMA to use internal data, external data, scenario analysis and BEICFs as inputs to its OR measurement system; however, it does not clarify the manner in which these elements should be combined to calculate the capital requirements. Therefore, the RTS set out standards for the supervisory assessment of key components of the OR measurement system, aimed at ensuring that the system is based on a well-founded methodology, effective at capturing the institutions' actual and potential ORs, reliable and robust in generating capital requirements and comparable across institutions.

With specific reference to the regulations established by the EBA, the RTS addressing the elements making up an institution's AMA framework are broken down into six chapters: General rules for the assessment methodology; Scope of OR; Qualitative standards—Governance and Operational risk management; Quantitative standards—Operational risk measurement; Insurance and other risk transfer mechanisms; Final provisions. Below we outline the contents of the five chapters (leaving out the last one on the transitional and final provisions of the

regime), anticipating the topics of the insights provided in other parts of this volume.

General Rules for the Assessment Methodology
For the purposes of assessing whether an institution complies with the requirements on documentation of the risk management system, authorities need to verify the quality and auditability of the documentation on the AMA (EBA 2015). In assessing the quality of the documentation, authorities need to verify that it be sufficiently detailed and accurate in order to allow the examination of the AMA by third parties and need, in particular, to verify the compliance with specific requirements.

Scope of Operational Risk
In order to assess whether an institution properly articulates what constitutes OR for the purposes of implementing policies and processes to evaluate and manage the OR exposure—as required by the CRD IV—authorities must verify that the institution identify, collect and handle data on OR events and losses related to legal, model and market risks.

Qualitative Standards—Governance and Operational Risk Management
This chapter is in turn divided into several sections: one dedicated to the principles of governance, a second to use test, a third to the audit and internal validation and the last to the data quality and IT infrastructure.

The Section Use Test states that the internal ORM must be closely integrated into an institution's day-to-day management process on a continuous basis and the AMA must be used also for internal purposes and to further enhance the institution's OR organization and control. Finally, the institution must demonstrate the stability and robustness of the AMA output by comparing the AMA own funds requirements to the capital requirements resulting from its previous regulatory regime (EBA 2015).

The data flows and processes associated with the ORM system must be transparent and accessible. To this end, the institution's data quality and the composite hardware, software and network resources and services required for the existence, operation and management of an IT infrastructure for AMA purposes must be appropriate. Particularly, the quality of the data used in the AMA framework must be maintained

over time, and the building and maintenance procedures must be regularly analysed by the institution, which must ensure also the soundness, robustness and performance of the IT infrastructures (EBA 2015).

Quantitative Standards—Operational Risk Measurement
The topic of quantitative standards is articulated in different sections: one on the use of the four elements (a sub-section focused on internal data), one on the core modelling assumptions of the OR measurement system, one on the expected loss and correlation, and one on the capital allocation mechanism.

Insurance and Other Risk Transfer Mechanisms
In order to assess the compliance of an institution with the requirements relating to the impact of insurance and other risk transfer mechanisms within an AMA, authorities must verify that the insurance provider meet the authorization requirements set out by the CRR (Article 323); that the institution avoid the multiple counting of risk mitigation techniques; that the risk mitigation calculation appropriately reflect the insurance coverage and that the framework for recognizing insurance be well reasoned and documented; that the institution's methodology for recognizing insurance capture all the relevant elements through discounts or haircuts in the amount of insurance recognition; finally, that the institution demonstrate that a noticeable risk mitigating effect is achieved with the introduction of the other risk transfer mechanisms (insights are discussed in Chap. 5).

The Four Elements of the AMA and the Other Quantitative Standards

In order to assess whether an institution is compliant with the AMA quantitative standards, the authorities must verify the institution is fulfilling the requirements referring to (i) the use of the four elements; (ii) the standards relating to the core modelling assumptions of the OR measurement system—and in particular—to its ability to capture tail events and the major drivers of risk affecting the shape of the tail; (iii) the standards relating to expected loss and correlation; (iv) the standards

relating to the internal consistency of the OR—Capital allocation mechanism (EBA 2015).

The Use of the Four Elements

The institution must produce internal documentation specifying how the four elements are gathered, combined and/or weighted. Such documentation must describe the modelling process that illustrates the use and combination of the four elements and the rationale for the modelling choices. To this end, authorities must verify that the institution have a clear understanding of how each of the four elements influences the AMA own funds requirements, and that the combination of the four AMA elements used be based on a sound statistical methodology (EBA 2015).

Authorities must verify that, for the collection or generation and treatment of the four elements, the institution apply all the criteria relating to internal data, external data, scenario analysis and BEICFs (EBA 2015).

For what concerns *internal data* (EBA 2015), the institution must implement in a clear and consistent manner the loss caused by the occurrence of an OR, before taking into account recoveries of any type (gross loss or loss); the occurrence related to the original loss that is independent of that loss and that is separate in time, in which funds or inflows of economic benefits are received from first or third parties (recovery); the recovery from insurers (insurance recovery) and the recovery from other parties (recovery except insurance).

Moreover, following an OR event—except when the OR event leads to a gross loss that is partly or fully recovered within five working days (rapidly recovered loss event)—the institution must be able to identify separately the gross loss amount, the insurance recoveries, and the recoveries without the insurance.

The institution also has to implement a system for defining and justifying appropriate thresholds, based on the gross loss amount and for identifying and collecting losses for management and measurement purposes (data collection threshold).

The data collection threshold selected by the institution for each level, such as the institution's organizational unit, the OR event type, the business line at which the institution's OR measurement system generates separate frequency and severity distributions (operational risk

category), must be reasonable and must not omit loss data that is material for effective OR measurement and risk management.

Lastly, for each individual loss, the institution must be able to identify and record in the internal database at least the date on which the OR event happened or first began (date of occurrence)—where available—the date on which the institution became aware of the OR event (date of discovery) and the date when a loss, or reserve, or provision against a loss was first recognized in the profit and loss (date of accounting).

Specific provisions on internal data are set out also with reference to the scope of OR loss, for the purposes of both OR management and calculation of the AMA own funds requirements. In particular, the OR loss must include the following items (EBA 2015):

- direct charges (including impairments and settlement charges) to the profit and loss account and write-downs due to the OR event;
- costs incurred as a consequence of the OR event including both external expenses with a direct link to the OR event, such as legal expenses and fees paid to advisors, attorneys or suppliers, and costs of repair or replacement to restore the position prevailing before the OR event, either in the form of precise figures, or, where these are not available, of estimates;
- provisions or reserves accounted for in the profit and loss account against probable OR losses including those from misconduct events;
- losses stemming from OR events, which are temporarily booked in transitory or suspense accounts and are not yet reflected in the profit and loss account (pending losses), and which are planned to be included within a time period commensurate to the size and age of the pending item;
- material uncollected revenues, related to contractual obligations with third parties, such as the decision to compensate a client following the OR event, rather than by a reimbursement or direct payment, through a revenue adjustment waiving or reducing contractual fees for a specific period of time in the future;
- negative economic impacts booked in a financial accounting period due to OR events impacting the cash flows or financial statements of previous financial accounting periods (timing losses), where they span more than one financial accounting year and give rise to legal risk.

Moreover, the institution must consider any additional items whenever they originate from a material OR event (EBA 2015). These include a nil loss caused by the occurrence of an OR event, such as an IT disruption in the trading room just outside trading hours (near-misses); a gain caused by the occurrence of an OR event (OR gain); an increase in costs or a shortfall in revenues due to OR events that prevent undetermined future business from being conducted, such as unbudgeted staff costs, forgone revenue, and project costs related to improving processes (opportunity cost); internal costs such as overtime or bonuses.

Excluded from the scope of OR loss are the costs of general maintenance contracts on property, plant or equipment; the internal or external expenditures to enhance the business after the occurrence of an OR event such as upgrades, improvements, risk assessment initiatives and enhancements, and insurance premiums.

Another standard related to internal data is linked to the need to guarantee that the institution record the loss amount generated by an OR event. Therefore authorities must verify that the whole amount of the incurred loss or expenses be considered as recorded loss amount for the purposes of both management of OR and calculation of the AMA own funds requirements, and in particular, that the recorded loss amount include all of the external expenses incurred as a result of the OR event, such as provisions, costs of settlement, amounts paid to make good the damage, penalties, interest in arrears and legal fees, unless otherwise specified.

To this end, the following requirements must be met (EBA 2015):

- where the OR event relates to market risk, authorities must verify that the institution include in the recorded loss amount of the OR items the costs to unwind market positions, unless the position is intentionally kept open after the OR event is recognized. Where the position is intentionally kept open after the OR event is recognized, authorities must verify that any portion of the loss due to adverse market conditions after the decision to keep the position open is not included in the recorded loss amount of the OR items;
- where tax payments relate to failures or inadequate processes of the institution, authorities must verify that the institution include in the recorded loss amount of the OR items the expenses incurred

as a result of the OR event, such as penalties, interest charges, late-payment charges and legal fees, with the exclusion of the tax amount originally due;
- where the OR event leads to a rapidly recovered loss event, authorities must consider appropriate that the bank count among the recorded loss amount of OR items only the part of loss that is not rapidly recovered;
- where there are timing losses, authorities must verify that the institution include among the recorded loss amount of the OR items all the external expenses incurred as a result of the OR event. Where the OR event directly affects third parties (e.g. customers, providers or employees of the institution) authorities must verify that the institution include in the recorded loss amount of the OR item also the correction of the financial statement.

The last issue concerning the internal data concerns the OR losses related to credit risk. For this purpose it is foreseen that the institution include—for the ORM purposes—within the scope of OR loss all the following: frauds committed by a client on its own account, occurring in a credit product or credit process at the initial stage of the lifecycle of a credit relationship (first-party fraud), and in particular inducement to lending decisions based on counterfeit documents or mis-stated financial statements, such as non-existence or overestimation of collaterals and counterfeit salary confirmation; frauds committed using the identity of an unaware person (third-party fraud), either occurring in a credit product or credit process (loan applications through electronic identity fraud—phishing—and using clients' data or using fictitious identities; fraudulent use of clients' credit cards by third parties).

In reference to *external data* (EBA 2015), in the case the institution participates in consortia initiatives for the collection of OR events and losses, the institution must be able to provide data of the same standard-fulfilling quality—in terms of scope, integrity and comprehensiveness—of internal data, and in agreement with consortia data reporting standards. The institution must also have a data filtering process in place, which allows the selection of relevant external data, based on specific predefined criteria. In order to avoid bias in parameter estimates, the filtering process must select data consistently regardless of the loss

amount, and—where the institution permits exceptions to this selection process–must have a policy providing criteria for exceptions and documentation supporting the rationale for those exceptions. Moreover, if the institution adopts a data scaling process involving the adjustment of loss amounts reported in external data (or of the related distributions) to fit the institution's business activities, nature and risk profile, the scaling process must be systematic and statistically supported and provide outputs consistent with the institution's risk profile. The institution's scaling process must be consistent over time and its appropriateness must be regularly reviewed.

The implementation of third AMA element, *scenario analysis* (EBA 2015), foresees that the institution have in place a robust governance framework relating to the scenario process that can allow it to generate credible and reliable estimates, independently from whether the scenario is used for evaluating high severity events or the overall OR exposure. To this end, authorities must verify that:

- the scenario process be clearly defined, well-documented, reproducible and designed to reduce as much as possible subjectivity and biases. Among these, the underestimation of risk due the small number of observed events (overconfidence bias); the misrepresentation of information due to the assessors' conflict of interests with the goals and consequences of the assessment (motivational bias); the overestimation of events with temporal proximity to the scenario assessors (availability bias); the distortion of assessments due to the categories within which the responses are represented (partition dependence); the bias towards information presented in background materials to survey questions or within the questions themselves (anchoring);
- qualified and experienced facilitators provide consistency in the process;
- the assumptions used in the scenario process be based, to the maximum extent, on the relevant internal data and external data with an objective and unbiased selection process;
- the number of scenarios chosen, the level of detail at which the scenarios are studied, and the units in which they are studied be realistic and properly explained, and that the scenario estimates take into account relevant changes in the internal and external environments that can affect the institution's OR exposure;

- the scenario estimates be generated taking into account in particular potential or probable OR events that have not yet, fully or partly, materialized in an OR loss;
- the scenario process and estimates be subject to a robust independent challenge process and oversight.

The last element of the AMA, the *business environment and internal control factors (BEICFs)*, must be forward-looking and reflect potential sources of OR such as rapid growth, the introduction of new products, employee turnover and system downtime. The institution must have clear policy guidelines that limit the magnitude of reductions in the AMA own funds requirements caused by BEICFs adjustments. The latter must be well justified and the appropriateness of their level must be confirmed by comparison, over time, with the direction and magnitude of actual internal loss data, conditions in the business environment and changes in the validated effectiveness of controls (EBA 2015).

Core Modelling Assumptions of the OR Measurement System

The institution must develop, implement and maintain an OR measurement system that is methodologically well founded, effective in capturing the institution's actual and potential OR, and reliable and robust in generating AMA own funds requirements. To this purpose, authorities must verify that the institution have appropriate policies on the building of the portion of data gathered (either actual or constructed) that fulfils the necessary conditions to serve as input to the OR measurement system to generate the AMA own funds requirement (calculation data set).

Another modelling assumption of the OR measurement system is that the institution apply the appropriate level of granularity in its model. To this end, the institution must take into account the nature, complexity and idiosyncrasies of its business activities and the ORs which it is exposed to, grouping together risks, sharing risk factors, and defining the OR categories of an AMA. The institution must justify its choice of level of granularity of its OR categories on the basis of qualitative and quantitative means, and classify OR categories based on homogeneous, independent and stationary data. The institution's choice of level of granularity of its OR categories must be realistic and must not adversely affect the conservatism of the model outcome or of its parts.

The institution must review the choice of level of granularity of its OR categories on a regular basis with the view to ensuring that it remains appropriate.

A third modelling assumption is that the institution has in place an appropriate process for identification of frequency and severity distribution of loss (loss distributions). The institution must follow a well-specified, documented and traceable process for the selection, update and review of loss distributions and the estimate of their parameters.

The last modelling assumption requires the institution to determine the frequency-severity aggregated loss distributions and risk measures in an appropriate manner. The techniques elaborated by the institution for that purpose shall guarantee that levels of precision and stability of the risk measures are appropriate, and that the risk measures are supplemented with information on their level of accuracy.

Expected Loss and Correlation

In the case an institution calculates the AMA own funds requirements only in relation to unexpected loss (UL), it must comply with specified requirements.

With regard to the assessment of standards relating to correlation, the institution must carefully consider any form of linear or non-linear dependence, relating to all the data, either to the body or to the tail, across two or more OR categories or within an OR category, which will then be verified by authorities.

Capital Allocation Mechanism

The institution's capital allocation mechanism must be fully consistent with the institution's risk profile and with the overall design of the OR measurement system; fulfilment of such requirements will then be verified by authorities.

3.4.2 Some Considerations on Advanced Methodologies

The adoption of advanced methods is generally associated with benefits such as risk differentiation among the Business Lines (BLs), the development of an OR sensitivity, the definition of appropriate capital

allocation policies, the setting of an active risk management, the pursuit of related objectives of efficiency and performance, as well as the saving of regulatory capital.

Such advantages, however, represent half the story; in fact, we must also consider the doubts and concerns related to the implementation of the AMA and their impact on the OR measurement and management systems. To a first approximation, the many critical issues relate to the high complexity of the models and the difficulties related to the incorporation of all four elements in the AMA framework.

Other criticisms concern the use of Value at Risk (VaR) , which is not fully effective at measuring risk when the returns do not follow a statistically normal distribution—as frequently occurs in OR. Furthermore, VaR provides an indication on the amount of risk, but not on its form of manifestation (legal risk, technological risk and so on).

Regulatory capital savings originated from the adoption of the AMA is another concern yet, raising questions on the validity of the reasons for the possible reduction of capital for the OR coverage in comparison with the more simplified approaches (BIA and SA).

Foremost we need to consider the opportunity of abandoning the assumptions of perfect correlation between BLs and event types. Despite the authorities having allowed the incorporation of estimates of the correlation between the operating losses in the calculation of capital requirement, there has been no appreciable uniformity in the approach adopted by intermediaries neither in terms of quantifying the dependence between BLs and event types nor in terms of the methods used to measuring that dependence.

Another open issue is the identification of appropriate techniques for the incorporation of insurance policies, such as OR mitigation tools that take into account the severity of the conditions for their eligibility (see Chap. 5).

According to some scholars, the only true reason that can explain the lower capital absorption resulting from the use of advanced models lies in the flexibility and discretion that the bank can follow in the construction of such models; hence a competitive disadvantage for the smaller institutions and the misalignment of the regulatory dictated to the objective of a level playing field.

These considerations—highlighting some of the AMA's weaknesses—point to the need of strengthening the elements of advanced

approaches. As for the standardized approaches, the suggestion here is not to limit action once the minimum level of compliance has been reached, but to continue in pursuit of the refinement of the different steps that lead to the construction and maintenance of the AMA. It is important to increase, within the LDC, the capability of representing both the current risk—through the effective identification of the multiple-effect and multiple-sequence events—as well as the potential risk, through the estimation of near-misses and opportunity costs. It is necessary to emphasize the contribution of the qualitative model of the analyses, and thus of the scenario analyses, evaluating the prospective risk factors (related to changes in the organizational, business and market profiles) and increasing the transparency and objectivity of assessments towards the benefit of their quality (for this latter aspect, an explanation of the most significant deviations between the subjective judgments and past evaluations and/or estimates originated from historical data might be necessary). The enrichment of the qualitative component may also arise from the optimization of KRIs, identifying those with better capacity for representation and prediction of OR. The model must feature (i) appreciable robustness, even in the face of adverse scenarios; incorporate the effects of correlation and risk mitigation, (ii) develop risk-sensitive allocation policies, and (iii) achieve a capital estimate that is properly balanced between the historical and the perspective component. Finally, special attention should be given to the enhancement of the use test, in order to be able to use the results of the model also towards strategic and decision-making purposes (e.g. the decisions on entering new markets or launch new products), to set the remuneration systems of the risk owners, and to develop fruitful forms of collaboration between the OR function and the internal audit.

3.5 Recent Regulatory Initiatives

Consistently with the overall supervisory focus on monitoring the implementation of OR standards, the Basel Committee has recently intervened in the field of OR on several fronts.

In the course of 2014, for example, it has reviewed the Principles for sound ORM (BCBS 2014).

As set out by the new principles, the Committee's expectations for the ORM include: all internationally active banks should implement policies, procedures and practices to manage OR commensurate with their size, complexity, activities and risk exposure, and seek continuous improvement in these areas as industry practice evolves. In order to enhance OR management, the principles provide comprehensive guidance regarding the qualitative standards that should be observed to achieve more rigorous and comprehensive ORM (for further detail see Chap. 4).

The Basel Committee has also reviewed the OR capital framework. Following an earlier consultation paper issued in October 2014, in March 2016 the Basel Committee proposed a new Standardized Measurement Approach (SMA) for OR (BCBS 2016a), as part of the broader objective of balancing simplicity, comparability and risk sensitivity. In addressing a number of weaknesses of the current framework, the consultative document focuses on the following key elements:

- the SMA will replace the three existing standardized approaches for calculating OR capital as well as the AMA and thus significantly simplify the regulatory framework;
- the revised methodology combines a financial statement-based measure of OR—the Business Indicator (BI)—with an individual firm's past operational losses. This results in a risk-sensitive framework, which also promotes consistency in the calculation of OR capital requirements across banks and jurisdictions;
- the option of using an internal model-based approach for measuring OR—the AMA—has been removed from the OR framework. The Committee believes that modelling of OR for regulatory capital purposes is unduly complex and that the AMA has resulted in excessive variability in risk-weighted assets and insufficient levels of capital for some banks;
- the proposed SMA framework shall be applied to internationally active banks on a consolidated basis. Supervisors will decide on the matter of application of such framework to non-internationally active institutions.

This proposal of reviewing the OR capital framework has inevitably generated second thoughts on Pillar 3 disclosure requirements,

and can be seen in the Consultative Document issued by the Basel Committee (BCBS 2016b), which takes into account the changes to the OR framework by proposing three new disclosure templates. Such templates should provide users quantitative data on historical OR losses, the drivers of a bank's OR charge under the SMA and details of a bank's incurred losses from ORs over the previous 3 years, respectively. In addition, further qualitative data on a bank's ORM framework would be obtained by the introduction of a new table.

3.6 Conclusions

Over the years the increasing importance of the OR has led the supervisory authorities to include such risk within the international capital adequacy framework (Basel 2 and Basel 3), providing alternative methods for calculating related own funds requirements. This regulatory initiative has marked an important step for the ORM, as it has given for the first time the impetus to the enhancement of the control of the bank's OR exposure. A convergence in terms of definition, scope and sourcing of OR has also been attained, with other positive impacts on the ORM practices.

However, the regulatory process is not yet complete: a further step towards completing the post-crisis reforms is needed. The current changing context has in fact underlined the need of a more rigorous and comprehensive ORM. To this end, a revision of the capital framework has also been proposed by the Basel Committee, aimed to overcome a number of weaknesses in the current rules and to ensure a better balance between simplicity, comparability and risk sensitivity.

Note

1. The European Banking Authority (EBA) must develop draft-implementing technical standards to determine the conditions of application of the principles for business line mapping and submit those standards to the European Commission by 31 December 2017.

References

BCBS (Basel Committee on Banking and Supervision). 2006. Basel II: International convergence of capital measurement and capital standards: A revised framework, Comprehensive version, June.

BCBS (Basel Committee on Banking and Supervision). 2011. Basel III: A global regulatory framework for more resilient banks and banking systems, revised version, June.

BCBS (Basel Committee on Banking and Supervision). 2013. Basel III: The liquidity coverage ratio and liquidity risk monitoring tools, January.

BCBS (Basel Committee on Banking and Supervision). 2014. Review of the principles for the sound management of operational risk, October.

BCBS (Basel Committee on Banking and Supervision). 2016a. Standardised measurement approach for operational risk—Consultative document, March.

BCBS (Basel Committee on Banking and Supervision). 2016b. Pillar 3 disclosure requirements—consolidated and enhanced framework—Consultative document, March.

EBA (European Banking Authority). 2013. Final draft regulatory technical standards on the conditions for assessing the materiality of extensions and changes of internal approaches when calculating own funds requirements for credit and operational risk in accordance with Articles 143(5) and 312(4)(b) and (c) of Regulation (EU) No 575/2013 (Capital Requirements Regulation—CRR), December.

EBA (European Banking Authority). 2015. Final draft regulatory technical standards on the specification of the assessment methodology under which competent authorities permit institutions to use Advanced Measurement Approaches (AMA) for operational risk in accordance with Article 312 of Regulation (EU) No 575/2013, June.

Krosner, S. 2008. Risk management and Basel II, speech at the Federal Reserve Bank of Boston, AMA Conference, Boston, May 14.

4

Operational Risk Management: Organizational and Governance Issues

4.1 Introduction

The centrality of the link between operational risk management and governance is underlined by the several cases of financial collapses, in which losses are mainly connected with supervisory and operational failure on behalf of the top management. Likewise, a sound operational risk management requires a focus on the organizational structure, in response to the need of combining measurement systems with efficient and adequate control units for managing operational risk.

In this chapter we analyse the organizational and governance issues related to the measurement and control of operational risk, focusing on the key functions involved (e.g., committee, OR functions), on the interrelationship between the OR function and other functions (internal audit and compliance) as well as on the role of reporting and information technology.

G. Birindelli and P. Ferretti, *Operational Risk Management in Banks*,
Palgrave Macmillan Studies in Banking and Financial Institutions,
DOI 10.1057/978-1-137-59452-5_4

4.2 An Overview of the Key Functions Involved in the ORM

Establishing a sound OR management entails the need for an in-depth analysis of multiple business processes and their components (sub-processes, phases and activities, according to an order of greater detail[1]). Such need is a clear sign of the strong influences exerted by OR on the organizational structure. On the other hand, it is also true that this structure—which is a key element of corporate defence strategies (Lyons 2006) and is often neglected in favour of the more commonly studied quantification issues—is crucial for healthy business management, as evidenced by many recent scandals arisen because of unclear reporting lines and ambiguous formalization of tasks and responsibilities.

The centrality of the link between OR and corporate governance is further highlighted by the recurrent cases of financial collapses reported in the "Facts on International Relations and Security Trends" (FIRST) database on operational loss events. In fact, the database identifies up to 62 crisis cases (Cagan 2006) in which losses that had mainly been associated to internal fraud were specifically linked to supervisory and operational failure on behalf of the board of directors and senior management. Accordingly, the focus on organization arises in response to the need of combining measurement systems with efficient and adequate control units for managing OR.

Traditionally, Internal Audit (IA) has coincided with the operational risk function, in that IA—together with the individual business areas acting as local and decentralized control units—has usually been the unit responsible for OR control and mitigation. Accordingly, IA can be compared to a sort of "ancestor" of OR function. Indeed, in many banks IA has taken on the leading role during the early stages of OR projects: the process of self-assessment of the internal control system facilitates the development of action plans and highlights right from the preliminary planning stage a multifunctional approach that assigns the direct responsibility of OR management to IA (Birindelli and Ferretti 2009).

Over time, the substantial overlap between IA and the OR function has been replaced by a clear separation of responsibilities and tasks, eventually leading to the independence of the two functions. However, the tendency to create a specifically dedicated OR unit featuring organizational collocation and operational levels mainly tailored around the size of the bank cannot be intended as an attempt to ignore the activity performed by IA: as we shall see, there are many synergies/forms of cooperation between IA and the OR function, such as the connections between control and ORs. Among these connections, the most evident and easy to understand, and closely interrelated, can be summarized as follows:

- ORs may reside in the weaknesses of the internal control system, considered as a whole or in its various components, including those components designed to safeguard other risks;
- exposure to ORs depends, among others, on the effectiveness and efficiency of the controls;
- controls are one of the management instruments and, as such, create value in the process of OR management;
- quality of control strategies is a key factor to address the intermediary towards more sophisticated and risk-sensitive methods of capital calculation;
- internal audit has extensive knowledge about OR factors (processes, Information Technology, human resources, etc.); in particular, it controls the reliability of the information systems—including automatic data processing systems—at the origins of technological risk;
- the qualitative component of the quantification method of capital (see Chap. 3) also includes a study on the activation of control procedures added to the existing ones (Miranda 2000).

In the guidelines for proper OR management, a broad description is dedicated to both IA and OR function, supported by the governing bodies.

Indeed, the roles of the different actors involved in the OR projects are extensively discussed by the BCBS in the "Review of the Principles for the Sound Management of Operational Risk" (BCBS 2014). Among

the tasks of the board of directors, the Basel Committee lists: approval and periodic review of the OR management system; approval of a governance structure with clearly defined responsibilities, in respect of the separation between the control and operational functions, in order to avoid conflicts of interest; and promotion (in conjunction with senior management) of an organizational culture giving maximum emphasis to effective risk management. The principles set out by the board of directors should be translated into policies, processes and systems for the various operating units of the bank. This task is assigned to senior management, which is also responsible for other duties, such as establishing clear hierarchical lines of authority and processes to monitor OR exposure.

The principles establishing precise responsibilities and duties of the board of directors and senior management can be summarized as follows (BCBS 2014):

- The board of directors and senior management should establish a corporate culture[2] that is guided by strong risk management and that is present throughout the whole organization (Principle 1: Operational risk culture).
- The board of directors should establish, approve and periodically review the framework for operational risk management and should supervise senior management to ensure that the policies, processes and systems are implemented effectively at all decision levels (Principle 3: Board of directors).
- The board of directors should approve and review a risk appetite and tolerance statement for operational risk (Principle 4: Operational risk appetite and tolerance).
- Senior management should develop—for approval by the board of directors—a clear, effective and robust governance structure with well-defined, transparent and consistent lines of responsibility. Senior management is responsible for consistently implementing and maintaining policies, processes and systems throughout the organization, which are designed to manage operational risk in all the bank's material products, activities, processes and systems consistent with risk appetite and tolerance (Principle 5: Senior management).

- Senior management should ensure the identification and assessment of the operational risk inherent in all material products, activities, processes and systems, in order to guarantee that the inherent risks and incentives are well understood (Principle 6: Risk identification and assessment).
- Senior management should ensure that there is an approval process for all the new products, activities, processes and systems that fully assess operational risk (Principle 7: Change management).
- Senior management should implement a process designed to regularly monitor operational risk profiles and material exposures to losses. Appropriate reporting mechanisms supporting proactive management of operational risk should be in place at the board, senior management, and business line levels (Principle 8: Monitoring and reporting).

The principal findings and recommendations relative to the principles concerning the activity of the governing bodies are shown in Box 4.1 (BCBS 2014).

Additionally, the Basel Committee envisages a process of independent review and challenge of the bank's operational risk management controls, processes and systems (this is the third line of defence[3]). Those who carry out such reviews must be competent and appropriately trained. Moreover, to ensure that the staff responsible for the control is independent, it must not be involved in the development, implementation and operation of the framework. This review may be done by the audit or by the staff independent of the process or system under review, but it may also involve suitably qualified external parties. In particular, internal audit should perform an independent review, so as to verify that the framework has been implemented as intended, is functioning effectively, meets not only the board-approved policies and procedures but also organizational needs and supervisory expectations. If audit activities are outsourced, senior management should consider the appropriateness of relying on an outsourced audit function as third line of defence.

The major principles for a sound management of OR are thus constituted by responsibility/culture diffused at the level of business unit, by

constant reviewing, continuous monitoring of risk exposure, and strong involvement of the governing bodies.

Box 4.1—Principles for the activity of the governing bodies: findings and recommendations from the BCBS (2014)

Findings

- ✓ A strong operational risk management culture has been implemented by the board of directors and the senior management of most banks.
- ✓ Forms of operational risk training, such as online modules, have been established in most banks. Nevertheless, many banks plan to enhance existing operational risk training.
- ✓ According to most banks, the board of directors has been active in supervising the control environments of the bank.
- ✓ According to most banks, the board of directors or a subcommittee (i.e. the risk or audit committee) was responsible for regularly reviewing and approving the Operational Risk Management Framework (ORMF).
- ✓ In some banks an operational risk appetite and tolerance statement is reviewed regularly and approved by the board of directors or by a delegated authority, while in other banks it is under development.
- ✓ Almost all banks have an independent and dedicated Corporate Operational Risk Function (CORF) to oversee the implementation of the bank's ORMF and also an internal audit group that has the responsibility of the third line of defence.
- ✓ The CORF is generally responsible for reporting all operational risk-related matters to the appropriate senior management/committees.
- ✓ Specific policies (viz. loss of data collection, risk and control self-assessment, key risk indicators, loss modelling, scenario analysis, etc.) that support the ORMF are developed by senior management and approved by the board of directors in most banks. In some banks, these policies are approved by the risk committee or operational risk committee of the board.
- ✓ There are some forms of coordination between the CORF and other risk management functions. There is room for improvement in the coordination activities. A noteworthy practice is the establishment of a regular meeting between the operational risk management function and other risk management functions to discuss issues and events, including boundary losses.
- ✓ In most banks, senior management has established an operational risk committee. It directs and coordinates the implementation of the ORMF.
- ✓ Risk and control assessments within the change management process for new products and initiatives are in a fully implemented stage in only about two-thirds of the banks.

✓ Many banks are fully compliant with the principle (n.8) related to regular monitoring and appropriate reporting, but some banks are planning to improve existing operational risk reporting, to ensure that the information is useful, concise and actionable.

Recommendations

Banks are encouraged to:

Board of directors

i. ensure that the scope of internal audit concern full implementation and execution of the ORMF, and not be limited to the operational risk capital model;
ii. ensure that the scope of internal audit include a review of the effective implementation and execution of the ORMF at the business unit or legal entity levels, in order to complement the overall audit of the ORMF; and
iii. consider the possibility of periodically engaging in a benchmarking analysis of the bank's ORMF, with the assistance of independent external advisors, as part of the bank's regular assessment of ORMF design and effectiveness.

Senior management

i. ensure that the ORMF be approved by the board of directors or by a board committee;
ii. ensure that the CORF have sufficient stature, resources and infrastructures, in relation to other risk management functions, so as to implement the ORMF;
iii. ensure that an operational risk culture be established;
iv. ensure that an effective independent challenge be applied by the second line of defence; and
v. further develop and implement operational risk training and awareness programmes.

The same bodies appear in the part of EBA (2015) dealing with the governance for the AMA institutions. In particular, to evaluate compliance with the requirements mentioned in Articles 74 and 85 of Directive 2013/36/EU and in Article 321(1), points (b) and (c) of Regulation (EU) No 575/2013, controls shall be conducted by the competent authorities on the work of the management body[4] and of senior

management.[5] For example, controls will assess whether the operational risk management process is appropriate and effective: in this respect, the competent authorities shall verify that the institution's management body discusses and approves the governance of operational risk, the operational risk management process, the operational risk measurement system, the operational risk tolerance[6] and the operational risk tolerance statement.[7] Moreover, the competent authorities shall verify that senior management play an active role, specifically that:

- it be responsible for implementing operational risk governance and a management framework approved by the management body and that it actually implement them effectively;
- it receive appointment from the management body to develop policies, processes and procedures for the management of operational risk and that it actually implement them effectively.

There is then a set of requirements to be respected, so that the operational risk management function be independent from the business units of the institution, as follows:

- acceptance of tasks (design, development, implementation, maintenance and oversight of the operational risk management process and of the operational risk measurement system; analysis of the operational risk associated with the introduction and development of new products, markets, lines of business, processes, systems; oversight of business activities that may give rise to an operational risk exposure that could breach the institution's risk tolerance), to be performed separately from the institution's business lines;
- appropriate commitment received by the management body and the senior management;
- absence of responsibilities for the audit function.

Also the head of the operational risk management function should satisfy precise requisites: adequate experience on operational risk; regular contact with the management body and its committees; independence from the operational units; active involvement in the definition of

the operational risk tolerance and of the strategies for its management and mitigation; assignment of a budget for the operational risk management function by the Chief Risk Officer (CRO) or by a sponsoring member of the management body in its supervisory capacity and not by a business unit or executive function. Finally, there shall be a control over an institution's reporting of its operational risk profile and of the management of operational risk: to this purpose, it will be necessary to check that reporting is regular, timely and sufficient and that it includes all the material aspects of operational risk management and measurement (see Sect. 4.5).

The information contained in the above-mentioned documents allows specifying the roles and responsibilities of the organizational structures and support units involved in the management of OR, primarily the OR function. This function is directly responsible for the OR management/control system, for the design and implementation of the relevant framework, for the development of the processes of OR identification, assessment/measurement, constant control and risk mitigation. Specific competencies can be identified in the field of risk transfer, measurement approaches, capital absorption calculation, allocation of economic capital, handling of change management by means of staff training programmes, specialized advice to decentralized units and loss identification. This latter requires the appointment of a person in charge as well as a Loss Data Collection (LDC) manager (at both group and individual company level), who should be distinct figures in accordance with the principle of functional contraposition between those who manage and those who control the census activities. The organizational structure of LDC should also include the support of subjects responsible for the census of losses by drawing from its own information archives.

Although some choices are not yet definitive, the trend is towards the creation of multiple levels of OR function operations signalling a horizontal type of expansion: the corporate-level structure is repeated in both business and service units, or it is replaced, still in the decentralized units, by one or more people in charge. Whatever the solution adopted in the decentralized structures, depending mainly on their size and risk exposure, there is a local management involvement

for an integrated and transversal approach to OR, in accordance with the very nature of risk. Indeed, if a centralized OR function is crucial for the joint management of OR, the "bottom-up" reports and proposals allow overcoming the danger of losing the capacity of analysis on risks that for their very nature are related to the activities of the business units (Brienza and Gianturco 2005). Integration between the two (top-down and bottom-up) approaches increases the quality of the information created, helps to prepare mitigation actions, and improves the efficacy of the evaluation tools. On the other hand, the assignment of OR ownership to decentralized units implies an alignment between OR ownership, profit centres, and those taking the risk. It also involves forming a hypothesis consistent with standardized approach mapping: "In the standardized approach of Operational risk capital charge, Basel Committee on Banking Supervision used the mapping principle based on business lines, which supports the assumption that the business lines own operational risk and are responsible for day to day management" (Pandey 2008).

4.3 Responsibilities and Tasks of Functions Dedicated to Measuring and Controlling Operational Risks

The allocation of roles in the multi-level OR management model implies the involvement of many banking structures. What follows is an indication of their principal responsibilities, moving from the OR committee to the OR functions (central and local).

4.3.1 The OR Committee

The OR committee can be an enactment of the risk committee: in such case the risk committee is divided into multiple specialist committees that are linked to the main types of bank risk and are diversified according to their fields of competency. One of the main tasks of the OR committee is to examine the outcomes of risk analyses and to put forward

proposals for mitigation (and later control the actions performed), interventions on the processes, and assessment of insurance coverage. The OR committee appears as a body of confrontation and sharing of ideas and proposals, with the representation of many competencies responsible for the management of the OR according to an aggregated vision. Basically, the OR committee plays a preliminary role, and has advisory and proposal-making functions.

The choice of establishing this committee corresponds to the needs of those who are responsible for the company functions involved in OR management to share moments of confrontation. The OR committee is the centre in which the functions responsible for the management of the risks related to their processes share an analysis of the risk profile: the OR functions play the role of "facilitators" (Bazzarello and Maucci 2009).

The mission of the OR committee is to support the company managers (or committees, like the risk committee), since it is, in general, responsible for:

- proposing interventions on the risks evidenced by the OR functions that have experienced operational events or that have an exposure to the ORs;
- recommending the insurance strategies and policies of the group, including renewals, limits and deductibles;
- reporting the information relative to the insurance policies signed within the group and to the insurance indemnities;
- analysing the reports on the operational risks;
- proposing control procedures and limits of operational risk-taking;
- monitoring the actions of risk mitigation.

Where required by the organizational complexity, it is advisable to set up a system of OR committees:

- a central committee (within the parent company) performing the functions of group committee of operational risks;
- a series of local committees in the main divisions/companies of the group.

This system will make it possible to obtain benefits in terms of economies of scope, as in the case of specialization of the local OR functions (see Sect. 4.3.3).

The role of the functions represented in the local committee does not differ from that of the members of the group committee. Instead, the local committee operates in a different perspective:

- the immediate objective is to support the company managers through both the analysis of the risk profile relative to the competence activities and the proposal of suitable mitigation actions, also in compliance with the decisions of the central OR committee;
- the mediated objective is to contribute in this way to the analysis and mitigation of the operational risk connected to the other segments of activities and to the group as a whole (Bazzarello and Maucci 2009).

The flow of information from the local committees to the central committee and vice versa guarantees the achievement of such objectives. The regulations inside the banking groups should provide that the local OR functions bring the proposals/analyses of the local committees to the attention of the central committee through the central OR function. It is the task of the latter to communicate the decisions of the OR group committee to the local OR functions so that these decisions can be discussed and shared by the local committees. The process is facilitated by the widespread participation of the main local operational risk managers to the OR group committee.

4.3.2 Central OR Function

The group OR function, also called central OR function, reports to the OR group committee. The function may be structured within the risk management area of the parent company and plays both a guiding and a coordinating role, which means that it mainly ensures consistency to the entire operational risk management framework. To this end, the central function performs analyses of group value, it defines tools and methodologies for the identification, assessment, control and

mitigation of the OR (with application to all the group companies), it is responsible for the measurement of the risks and of the related capital requirement at the consolidated level, and also of the internal capital for Internal Capital Adequacy Assessment Process (ICAAP) purposes.

Furthermore, the central function may establish tolerance thresholds to the OR for the various business units, it may (or may not) provide support in the choice of insurance coverage, and may contribute to the estimation of risky exposure in case the group enters new sectors of the market and/or develops new products. Basically, the OR function in the parent company stands out for its peculiar responsibilities in terms of guidance and coordination, typical of the central functions and aimed at ensuring an efficient application of the operational risk management framework, defined at group level, by the companies of the group. When carrying out its activities, the central OR function coordinates with the OR functions/control units in the group's banks: these latter can be articulated at multiple levels (company or local, decentralized and specialized) (see Sect. 4.3.3).

Therefore, the central OR function establishes the guidelines and plays a role of support and control in relation to the OR functions present in the group's companies. The ultimate goal is to verify the implementation of the procedures and methods for OR evaluation, and thus the central OR function receives relevant information and reports from the local OR functions in order to perform such evaluation (Bazzarello and Maucci 2009).

In particular, the central OR function is responsible for:

- defining common standards for all the group's companies about the control of operational risks;
- developing models to measure operational risk;
- measuring operational risk capital at group level;
- checking that the data of operational loss are regularly collected and stored in the OR database of the group;
- controlling exposure to the operational risks of the parent company and of the group with the support of the OR company functions, monitoring risk indicators and regularly performing scenario analyses;

- proposing to the parent company OR committee risk thresholds for both the parent company and the group, with the support of the OR company functions;
- creating a regular flow of information towards the parent company on the exposure of the group to operational risks, with the support of the OR company functions;
- proposing to the parent company's OR committee mitigation actions against the exposure to operational risks, with the support of the company's OR functions;
- advising on handbooks related to OR management drafted by the group's companies before they are submitted to the approval of the company's board of directors;
- suggesting the parent company's OR committee insurance coverage to mitigate the exposure to operational risks and supporting the group's companies in the definition of the types of coverage;
- assessing and proposing coverage, in forms other than insurance, to mitigate OR exposure;
- creating relations with the supervisory authorities and the relevant international institutions on issues of measurement and control of operational risks;
- providing regular training on operational risks to the OR functions of the group companies;
- defining the functional requirements of the application package implementation at group level to support operational risk control.

4.3.3 Corporate OR Function

An efficient management system of operational risk requires the setting up of an OR function in each company of the group (local OR function). The aim is to obtain an appropriate extension of the application perimeter of the operational risk management framework. The risk governance system should also envisage functional reporting of these local functions to the central OR function.

Within the framework of a markedly divisional business model, the corporate structures focus their activities on a specific business (e.g. retail, corporate, investment banking, leasing, consumer finance, asset management, etc.), or service (information technology, back office, logistics, etc.). Therefore, the divisional model facilitates the development of specific skills on behalf of the local OR function. This allows an effective adaptation of the operational risk management framework related to 'local requirements', in their different dimensions: business types, geographical features like the local regulatory peculiarities, dimensional scale and so on. Functional reporting of the local OR function to the central OR function ensures a consistent application of the framework within the group.

The set of OR functions thus constitutes a specialized network that ensures effective risk monitoring and a timely flow of information to the company managers, both local and central. In particular, each OR function, including that of the parent company for its role of operational risk manager of the 'Holding Bank', is responsible for the following activities (Bazzarello and Maucci 2009):

- controlling exposure to the operational risks of the company, in compliance with the standards and procedures defined by the group's policies on OR management;
- verifying that the operational loss data are regularly recorded in the OR database of the group;
- periodically providing the data on operational risks (internal losses, risk indicators, scenario analysis, produced reports and action plans) to the central OR function;
- proposing processes, tools and models for the control of operational risks to the respective OR committee and to the central OR function;
- checking compliance with the risk limits, promptly informing the managers, internal audit and the central OR function in the case these limits are exceeded;
- identifying and collecting the risk indicators, performing the scenario analyses and ensuring the quality of the collected data with respect to the group standards;

- collaborating in the analysis of the impact of the operational risks on the introduction of new significant products and on the implementation of significant changes either in the activities carried out or in the structure's organization;
- checking that the company is equipped with business continuity plans and that these are regularly tested and updated;
- offering insurance policies to cover the operational risks faced by the company, in collaboration with the central OR function;
- proposing plans for operational risk mitigation, including insurance coverage, and informing the OR committee of the company (if any), the board of directors and the central OR function;
- producing regular reports on exposure to the operational risks of the company (losses, indicators, scenarios) for the company managers;
- providing the company structures with regular training on the control of operational risks;
- keeping relations with the supervisory authorities and with the relevant local institutions on the issues of measurement and control of the operational risks.

The company may include OR managers at a more granular level, namely at business unit level, with which the local OR function interacts and collaborates. These levels of managers are often identified as the OR officers. The tasks performed by these managers allow an OR management at decentralized level. The most common tasks include the following (Birindelli and Ferretti 2009):

- managing of the loss data collection process within the business unit (then transmitted to the OR function of one's company);
- constant monitoring of the census of loss data to ensure utmost completeness;
- participating in the assessment process in many respects: preparatory meetings with the subjects in charge of evaluation, support the conduct of assessment, checking the completeness and consistency of the answers, contribution to the examination and interpretation of the results, sharing of corrective actions and of the relative priorities in relation to the identified risks;

- adequate and detailed reporting on the business unit's level of risk exposure to managers/persons responsible for the business unit;
- disseminating throughout one's business unit an adequate risk and control culture, which should go beyond training on purely technical issues and aim at sharing objectives of OR management, transmitting a common language and valorising everyone's contribution towards the achievement of the expected results. Such activity of raising awareness, which also (and especially) involves the top managers, may combine the issuing of handbooks to specific classroom and web-based training sessions, or to more advanced training approaches, such as interactive portals;
- being involved in the definition and implementation of mitigation strategies, i.e. methodological support to the organizational units for the implementation of possible actions of mitigation of risky exposure, considering the critical and vulnerable issues detected in one's business unit (e.g. obstacles to the achievement of objectives, areas of improvement, control deficiencies, etc.);
- systematic updating of the business unit, taking into account the development of the OR management framework. In this context, the OR managers should provide suggestions for improvement in terms of methods, standards, processes and applications;
- supporting the risk owners of the main processes, who are required to report true and/or estimated risk events due to the action of OR factors identified while performing daily activities and relating to the processes monitored.

An active operational risk management in the business lines as 'first line of defence' requires adequate communication between the various business lines and the operational risk experts (Milkau 2013).

The OR management organizational model also involves structures, transversal to the entire bank—known as the specialized OR officers—informing about the risks under their own responsibility and suggesting risk mitigation actions. Among these OR officers there are the following: Physical Safety, Information Safety, Legal Department, Human Resources, Logistics, etc.; in other words, those who manage mitigation

of the risk related to specialized units, designed to establish a targeted action plan for each risk factor.

Therefore, the OR internal governance may include functions/officers with different operational levels. In particular, we can distinguish among the group (or central) OR function, company (or local) OR function, decentralized OR officer and specialized OR officer. An example of allocation of roles to the four levels identified is included in Table 4.1 (Metelli 2005).

Table 4.2 summarizes the main tasks and responsibilities of the governing bodies and of the OR function, as well as the roles of the chief risk officer and of the OR committee—if present, otherwise of the risk/audit committee (Prokopenko and Bondarenko 2012).

4.4 Interrelationships Between the OR Function and Other Functions

The company functions with which the OR function relates can be classified as control functions, support functions and business functions.

The control functions are the central management functions that have control responsibilities. The most important for our purposes are internal audit and compliance (see Sect. 4.4.1). The control functions are different from the support and business functions since they do not manage the operational risks directly.

The support functions are those that provide services to the business and control functions. Some are central management functions, present at local level; others are functions centralized in specific companies which typically provide centralized information, administration and logistic services ("service companies"). The former include the legal function, the human resources function, the organization function and the safety function. The relationship between the OR function and the business continuity function deserves to be further studied, owing to the role of the latter in the context of mitigation of the operational risks (see below).

Table 4.1 Tasks of OR functions/officers (Metelli 2005)

Risk Management in the parent company	Group OR Function	Implements the methods for detecting, assessing, mitigating and controlling the ORs to be applied to the group companies, ensuring efficacy and consistency with the strategies and policies approved by the board of directors. At group level, supervises loss detection and risk measurement, and generates flow of information useful both inside and outside the group. Proposes modes of intervention for monitoring and mitigating the ORs. Acts as coordinator with company OR functions, decentralized OR officers and specialized OR officers.
Group Company	Company OR function	Is the supervisor and the person responsible for the management process of the ORs within the company and checks that it is working properly. In the fulfilment of their activities, coordinates with the group's OR function and with the decentralized OR functions within the company. Participates in the OR committee.

(continued)

Table 4.1 (continued)

Business Units	Decentralized OR Officer/ Process risk owner	Provides operational supervision of the OR management process within the business unit, by coordinating and supporting the risk owners of the main processes. Supports the monitoring process of the risks and participates in the definition and implementation of the mitigation strategies. Coordinates with the company OR function in executing its functions. The risk owner's task is to recognize and notify harmful events, either actual or potential, related to OR factors identified in the processes monitored directly during the daily activities. Participates in the execution of the mitigation interventions, and coordinates with the decentralized OR Officer for his/her activities.
Security, Information Security, Complaints, Human Resources, Legal, and Logistics Department	Specialized OR Officer	Provides operational supervision of the performance of the OR management process within its specialized unit. Supports the risk monitoring process and participates in the definition and implementation of the mitigation strategies. Coordinates with the company's OR function in the execution of their functions.

Table 4.2 OR Governance internal structure (Prokopenko and Bondarenko 2012)

Element	Tasks and responsibilities
Supervisory board	Approves and periodically reviews the operational risk management strategy; Receives reports on OR exposure against risk appetite; Is aware of major ORs and significant losses; Ensures that the management board carries out its responsibilities
Management board	Is responsible for implementing the risk management strategy; Approves and periodically reviews the operational risk framework; Ensures that the staff in organization is aware of its role in OR management; Ensures that appropriate action is taken in response to OR exposures exceeding the appetite; Launches and manages projects for operational risk management (including budgeting, resourcing and awareness campaign)
CRO (often a board member)	Is responsible for implementing the OR framework; Provides risk leadership, vision and direction; Develops a supporting infrastructure; Monitors the operational risk project; Manages internal OR knowledge; Oversees/controls OR management
OR function	Implements the OR management framework; Creates management tools (risk policy, monitoring, assessment, systems, methods); Issues guidelines and methods for OR management; Identifies, assesses and analyses key risks; Monitors risk exposures against risk appetites
(Operational) Risk/Audit committee	Addresses high-level technical issues; Monitors implementation of risk policy and strategy; Takes measures to improve quality of risk management; Reviews the results of the risk assessments and makes recommendations on OR matters

Finally, the business functions process and distribute products and services to customers using the services provided by the support functions.

The interdependencies and complementarities that can be identified between the OR function and other functions require a formalization of duties through internal rules, group regulations or other modalities. This formalization serves to delimit the border of their responsibilities and to avoid the possible overlap of roles.

In addition to the functions that will be discussed below (see Sect. 4.4.1), the main functions involved in the management of OR are listed below:

- Risk Management (RM) is involved especially in the development of calculation methods, with subsequent control by the auditors with regard to the procedural aspects and to the measuring tools. RM is basically called to handle the quantitative component of the OR management framework, and especially the LDC and quantitative processing of risk self-assessment findings. The border between the RM and the OR function must not, however, be interpreted as a clear separation between the two: the former, in fact, is often a second-level control function on market, credit and operational risks. Indeed, the structure responsible for OR management is often part of the RM.
- Organization, in the role of mitigation manager, contributes to reengineering the business processes with the objective of reducing risk exposure and implementing/consolidating preventive controls which focus on the processes themselves. Accordingly, being the key actor within the formalization of the work processes, the organization defines and updates such processes with the aim of monitoring the risks.
- Legal function is actively involved in the identification and assessment of the legal risk embedded in the OR; it also monitors relevant indicators such as customer complaints, insurance compensations and revocatory actions.[8]
- Planning and Control: contributes especially to the definition of the budget objectives and of the long-term plan. In so doing, it assesses OR events due to bank policies and strategies, takes into account

information and guidelines coming from other functions and governing bodies, in order to integrate the plans with the capital plan during the internal capital adequacy assessment process.

The regulatory authorities request that the financial institutions define a business continuity plan aimed at ensuring continuity of the company's operations in the case of service interruption.[9] The plan must enable the financial institutions to maintain and restore operations in the occurrence of unpredictable events that may impact on business continuity. Within the framework of the OR management, the business continuity plans thus constitute one of the three pillars for OR management, alongside the measures for revision of the operational processes and of the control systems and risk-outsourcing policies (e.g. insurance coverage).

Verifying that the institutions have in place adequate and updated plans for operational continuity falls within the specific tasks of the OR function. Therefore, the business continuity function is a strategic partner for the OR function towards the actual implementation of the operational risk management system.

Each institution must define a business continuity plan based on the risk exposure of its activities, by applying technical analyses such as business impact analysis, analysis of business continuity requirements and risk assessment. In this process it is fundamental to identify the resources and functions that must be reactivated in case of service failure. Hence, the business impact analysis performed by the business continuity function represents an extremely relevant step in the phase of definition of the business continuity plan. The OR function is, in turn, a strategic partner of the business continuity function to integrate the information useful to the business impact analysis.

4.4.1 Interrelatedness Between OR Function and Internal Control System

The performance of the internal control system is expressed in terms of adequacy and compliance; therefore, the internal controls are assessed for their effectiveness (independent of their application) as well as for their correct implementation (Gusmeroli and Bonolo 2009).

The recognition of adequacy is directly linked to the type of control, i.e. to the capability of the control to monitor risk effectively/efficiently. The main factors relevant for this evaluation include organizational adequacy of the structure in charge of the control, the type of control (automatic or manual; preventive or final), the frequency with which it is performed, and its traceability (intended as accountability). As a general rule, the adequacy of controls is then assessed by comparing the existing controls with the so-called virtuous/benchmark controls, which are intended as effective controls, which can either (or not) be foreseen by the institute and which minimize the potential risk to a minimum or acceptable level. Conversely, the assessment on compliance is drawn from direct establishment of the person who has made this control (the internal subject responsible for performing it or not).

The methodological approach thus allows to start from a "potential" risk, i.e. "gross" of controls (independent of the effectiveness of the existing controls), and end with a "residual" risk, i.e. "net" of controls. Residual risk expresses the qualitative assessment of the risk to which the bank is exposed, keeping into account the existing controls. Hence the evaluation of residual risk is achieved through a self-risk assessment process, which largely involves those who are responsible for the processes examined from time to time.

This approach, however, needs to be aligned with the company's evolution through the addition of dynamic components that are capable of capturing the trend of the risk profiles over time. Basically, the elements of dynamism can be identified as (i) performance indicators or indicators of possible anomalies (KRI—key risk indicators), (ii) compliance control outcomes (checklist of controls/compliance testing), and (iii) self-assessment questionnaires (Gusmeroli and Bonolo 2009). In detail:

1. KRIs allow to observe the dynamics of risk over time. These indicators thus enter the evaluation process of residual risk and allow reducing the typical subjectivity of qualitative assessment, since the residual risk is also obtained—thanks to the KRIs—on the basis of objective/empirical indicators. KRIs can thus be used as qualitative correctors of residual risk, showing a plus or minus of the residual

risk on the basis of variation of their value during a given period of time;
2. checklists are a key information component that allows one to verify that the controls are adequate and implemented: the audit's checklist provides feedback on the actual application of the control mechanisms;
3. finally, questionnaires allow to engage the process owners on a regular basis and enquire on whether the initial findings are still current and on whether there have been any organizational/operational changes that may have affected the previously identified and assessed risks. Moreover, for each risk/process detected in a specific operational area, the experts must do a new estimate for the expected loss, in terms of frequency (e.g. frequency of the event over the year) and severity (e.g. average amount of loss per unit). Self-assessment of the risk through the opinions of experts is therefore a useful tool to test the evaluations conducted in the preliminary phase.

Hereon, the discussion on the relationship between OR and the internal control system will focus on the interrelatedness between the OR function and internal audit, and then move to the relationship with the compliance function.

Relationship Between the OR Function and Internal Audit

Internal audit is another actor within the operational risk governance; its role is divided into the following phases (Fernández-Laviada 2007):

- Operational risk identification
- Operational risk assessment (Qualitative evaluation and Quantitative evaluation)
- Operational risk mitigation
- Monitoring and reporting operational risk.

In particular, internal audit participates in the OR management process, by contributing on several fronts (Bazzarello and Maucci 2009; Birindelli and Ferretti 2009); namely, it:

- checks the quality of business processes and operational and computer-based procedures;
- assesses the adequacy of internal controls both at the level of business lines and of the support units and controls them on the basis of the results of loss data collection;
- may cooperate with the organizational structures responsible for the design, development, implementation and maintenance of the operational risk control system and of its process of self-evaluation, although the responsibility for developing a system for the operational risk control remains exclusively bestowed on the competent organizational structures;
- judges the effectiveness of both the internal control system and any corrective actions to reduce risk exposure. When assessing the adequacy of the OR control system, internal audit is responsible for reviewing the functionality and effectiveness of the system and its conformity with the regulatory requirements;
- intervenes directly on one of the events causing operating losses (internal fraud), in its role of controller of ethical conduct, especially that of employees;
- performs periodic checks on the quality, completeness and integrity of the elements of the measuring system (including assessments on the adequacy of the internal validation process and on the use test), despite not being actively involved in measuring OR;
- is, lastly, a reference point for the OR function; in fact, the OR function may ask the auditor to analyse, measure and assess the operational risks. In particular, audit reports are a useful source of information for identifying operational risks in the processes that must be controlled by OR indicators or be assessed by scenario analysis. Internal audit's suggestions on how to compensate for the deficiencies of the processes can be the basis for the development of operational risk mitigation plans.

If internal audit's contribution to the process of OR management during the phases of monitoring/reporting and of control/risk reduction is important, its role in the earlier phases (identification and assessment) appears just as relevant. Indeed, with reference to identification,

the internal audit contributes to defining criteria of risk identification, mapping risks/processes and selecting the databases in which the operational losses are collected. Furthermore, internal audit analyses the quality of the documentation that supports the OR identification process and verifies, in terms of time and of form, the consistency and integrity of the process.

The most significant activities for the implementation of the second phase (assessment) are represented by IA's contribution to drafting self-assessment, writing reports useful for evaluation of internal control factors (integral part of one of the AMA components[10]), performing analyses aiming to identify audit priorities and verify the coherence between risk profile on the one hand, and objectives of the governing bodies, on the other (Scoppio 2005).

Hence, although the independence between the OR function and internal audit is respected, there is a complex and rich flow of information between the two functions (Garnero 2003), as summarized in Fig. 4.1.

With specific reference to the AMA institutions, EBA (2015) establishes that an institution's audit and internal validation functions have to confirm, on a regular basis, that the operational risk management and OR measurement processes implemented for AMA purposes are reliable and effective in managing and measuring operational risk within the organization. Furthermore, an institution's audit and internal validation governance must be of a high quality.

With regard to the first point, the audit function must verify the integrity of the operational risk policies, processes and procedures, assessing whether these comply with legal and regulatory requirements as well as with established controls (at least on a yearly basis), with emphasis on the verification of the quality of the sources and of the data used for operational risk management and measurement purposes. Moreover, the audit function must have in place a review programme that is regularly updated in reference to (a) the development of internal processes for identifying, measuring and assessing, monitoring, controlling and mitigating operational risk; (b) the implementation of new products, processes and systems that expose the institution to material operational risk. It is also important that the internal or external audit

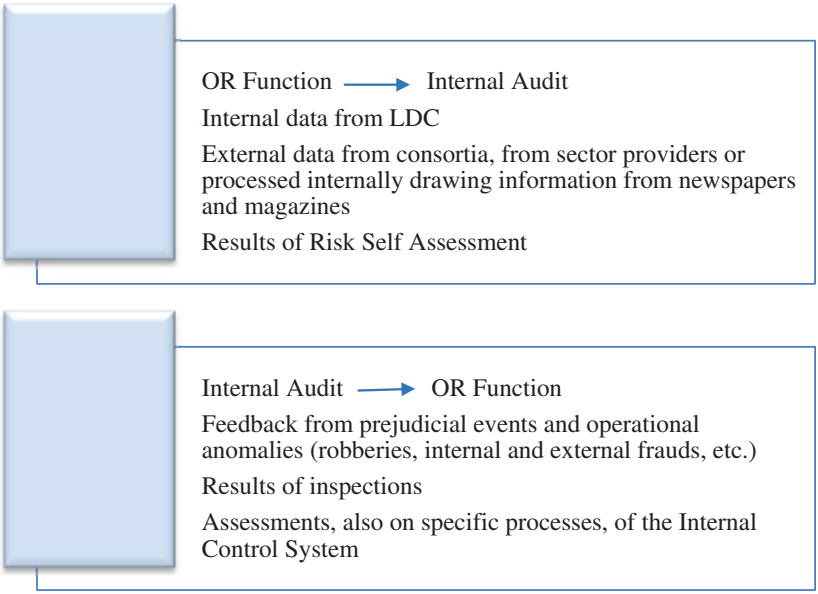


Fig. 4.1 Example of information flow between the OR function and internal audit (Garnero 2003)

functions be independent of the process or system being reviewed and that, where audit activities are outsourced, the management body and senior management of the institution remain accountable for ensuring that outsourced functions are performed in accordance with the institutions' approved audit plan.

Finally, with regard to the second point, the evaluation of the audit governance requires that the audit programmes for reviewing the AMA framework cover all significant activities that could expose the institution to material operational risk, including outsourced activities.

Relationship Between the OR Function and the Compliance Function

Acknowledgement of the contiguity between the OR function and the compliance function goes back to some years ago, when the Basel Committee recognized "a close relationship between compliance risk

and certain aspects of operational risk" (BCBS 2005). This statement is confirmed by numerous pieces of evidence: thus, it emerged that 75% of third level event types for classification of operational risk refers to compliance issues (Renna 2007); likewise, two Italian associations (Associazione Bancaria Italiana - ABI and Database Italiano Perdite Operative - DIPO) deemed the coverage of compliance risk net of reputational risk unnecessary, as the events at the origin of this compliance risk subset are included in the sources of operational risk (Pasquini 2009). Even the reading of the banks' balance sheet shows that the two risks are often not dealt with as stand-alone categories: it is not infrequent to find compliance risk in operational risk, as a component of the latter.[11] At the same time, there are now initiatives to exploit synergies in terms of database and assessment approaches (Berlanda 2009). From a sample of operational risk event types, it is indeed possible to go back to those more directly referable to compliance risk, after adjustment and screening operations (e.g. the exclusion of "pure" operational risk events—natural catastrophes, external frauds and other external events; those with date of occurrence prior to the enactment of regulations currently in force, and those without material loss).

The main interaction concerns the mutual improvement in the risk assessment systems. Besides, the presence of common risks allows the compliance function and the OR function to set up effective forms of collaboration. For example, the former may help to control the operational risk management system, to collect the loss data and to carry out the risk self-assessment. The latter, instead, may support the compliance function in the mapping of processes and in the reporting on time series of data and on risk exposure (Birindelli and Ferretti 2008).

In terms of specific areas of responsibility, synergies may involve systems for risk identification and measurement, which require periodic and structured information flows between the two functions (see Fig. 4.2 for a summary).

The compliance function therefore transmits to the OR function judgments on the controls concerning operational and compliance risks; it contributes to the integration of loss data collection through an analysis of the sources of compliance risk; it supports the drawing up of risk self-assessment by means of its qualitative evaluations and interviews of

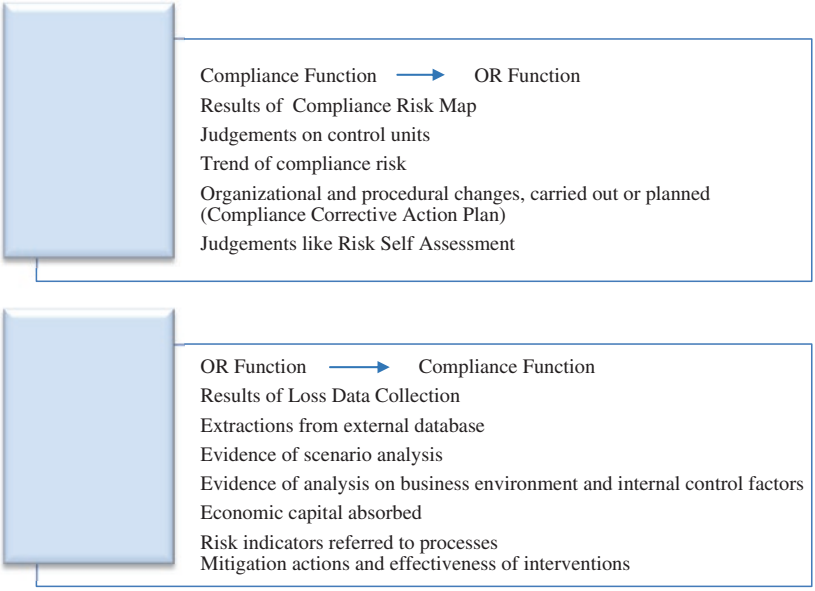


Fig. 4.2 Example of information flow between compliance function and OR function (Birindelli and Ferretti 2013)

risk owners; it informs on the trend of compliance risk and mitigation interventions carried out and planned.

By contrast, the OR function activates flows especially on events of operational loss linked to compliance issues, so that it can support the drafting of the compliance plan. It also supports risks and process mapping, revision of the existing controls, monitoring of the measures taken by the compliance function in terms of adequacy and effectiveness, definition of the procedures and drawing up of the methods used to measure compliance risk that impacts on reputation. Specifically, the OR function extracts and sends loss data (internal and external), results of scenario analyses and evidence of analysis on business environment and internal control factors; data on the absorbed economic capital; risk indicators useful for monitoring processes involving compliance risk;

reports on actions of mitigation and their effectiveness (Birindelli and Ferretti 2013).

4.5 Reporting on Operational Risks

The system of reporting on operational risks must ensure an adequate level of information on the operational risks through the exploitation of the tasks carried out by the OR functions, the company managers, and the dedicated committees. The information flow can be considered appropriate when this assumption takes place at all the levels of bank organization: process owners, managers at corporate and centralized level, senior management at group level, boards of directors at the corporate and parent company level (Bazzarello and Maucci 2009).

The corporate OR functions should regularly produce reports on the exposure to operational risks to submit to the company managers and to the competent local committees. For both the group and the parent company such responsibility is on the centralized OR function. The corporate OR function should periodically prepare a report for senior management and for the competent committees in which the exposure to operational risks, mitigation actions and capital at risk are analysed. These reports, which should be promptly submitted to the centralized OR function, are based on (Bazzarello and Maucci 2009):

- Trend of operating losses, of insurance recoveries and of risk indicators;
- Results of scenario analyses;
- Significant operational events (both internal and external) corresponding to the period of reference;
- Capital at risk and proposed mitigation actions.

The sharing of reports within the corporate OR committees is essential: it allows making all the information available, ensuring an adequate support to the corporate decision-making process. Similarly, the

information flow towards the centralized OR function and the group OR committee ensures an adequate support to the decision-making of the parent company's senior management and board of directors. In support to such "adequacy" (i.e. timeliness and quality of the data, also in terms of informative value), it is essential that OR managers create a system of relationships that get the risk analyst closer to the risk, by means of a preferential relationship with those in charge of the control, support and business processes.

In banking practice (BCBS 2014), the OR functions of many banks have established adequate operational risk reporting and there are often data repositories that allow for the central capture, aggregation and reporting of key operational risk data (operational losses, operational risk assessments, control deficiencies and key risk indicators). However, some banks are currently self-assessing their operational risk practices against the Basel Committee's "Principles for Effective Risk Data Aggregation and Risk Reporting" (BCBS 2013). These banks recognize the benefits of improving their risk data aggregation capabilities and risk reporting and are working towards this goal. In particular, they are aiming to improve completeness and timeliness of data, and to enhance the current operational risk data reconciliation processes and the flexibility of operational risk reporting through improved ad hoc reporting. Furthermore, many banks state they have implemented quality-sensitive data reporting systems (in terms of comprehensiveness, accuracy, consistency and appropriateness of volume), which are timely[12] and periodically submitted to review (BCBS 2014).

For AMA institutions, EBA (2015) states that the competent authorities shall verify the timeliness, accuracy, relevance and comprehensiveness in identifying problem areas of the institution's reporting systems and internal controls (Article 11). To this purpose, the competent authorities shall in particular verify that:

1. the reports be distributed to appropriate levels of management and to areas of the institution that the reports have identified as areas of concern;
2. the institution's senior management receive reports at least on a quarterly basis, reflecting the up-to-date status of the institution's

operational risk profile and use these reports in the decision-making process;
3. the institution's operational risk reports contain relevant management information and at least a high-level summary of the top operational risks of the institution and of the relevant subsidiaries as well as business units;
4. the institution use ad hoc reports in case of certain deficiencies in the policies, processes, and procedures for managing operational risk in order to promptly detect and address these deficiencies and therefore substantially reduce the potential frequency and severity of a loss event.

Therefore, the competent authorities shall oversee that the AMA institutions adopt effective risk reporting systems, which are a prerequisite of sound internal governance. These systems shall involve not only the management body and senior management, but also all the functions responsible for the management of operational risks to which the institution is, or might be, exposed.

4.6 Operational Risk and Information Technology

Information technology has a double nature, representing simultaneously both an element of risk and a factor of mitigation. IT can represent an element of risk since it can constitute the triggering of the technological risk and thus of the loss events linked to malfunctions and errors in the information systems, or linked to business disruptions. It may also represent a source of indirect risk which occurs, for example, in the case of unskilled personnel using technological applications. On the other hand, information technology constitutes a factor of mitigation since it supports the implementation of risk control actions, and the establishment of contingency plans, including the redesign of the company processes. Accordingly, because of this double nature, strengthening of the technological equipment amplifies safety

and reliability issues of the application systems, thus increasing the elements of vulnerability to which the bank is exposed.

4.6.1 IT as a Risk Factor

IT risk is a key component of operational risk, mainly through two event types (or subcategories). One is the so-called "business disruption and system failures" type, which addresses the disruption of regular business due to system failures, while the other type is "external fraud", which covers threats from external parties trying to hack into a company's systems and computers (Friedhoff and Mansouri 2015).

The major classes of risk associated with IT and, in particular, with network operations are (Paessler 2014):

- Technology risks: these are traditional IT concerns ranging from equipment failures through network-borne computer viruses and worms to more exotic issues such as denial-of-service attacks, intrusion attempts and "war walkers" accessing wireless networks from outside the building;
- Legal and personnel risks: these include compliance issues such as preparing for possible legal discovery requirements which might include email collection for civil suits; employees downloading inappropriate material from the Internet which could create hostile workplace suits; and potential sabotage or espionage by employees;
- Natural and man-made disasters: floods, earthquakes and large storms, while much less likely, their occurrences can be devastating. Defining adequate strategies for managing these risks is one of the most difficult tasks of risk management.

In the case of a company producing IT services, typical operational risks are as follows (Giardina and Ierardi 2009):

- Defects of the applications produced due to shortcomings in the testing phases
- Delays in the production of applications due to testing inefficiencies

- Errors, omissions or delays in the transition into production of software
- Breach of confidentiality rules
- Purchase of software not compliant with quality, cost-effectiveness or performance criteria
- Inadequate integration of new functionalities of the software developed, or regression of functionalities
- Lack of adequately skilled human resources
- Fraudulent use of logical accesses
- Unauthorized external access to business systems
- Unauthorized access to sensitive areas
- Uncontrolled access during unattended timeframes
- Lack of tools to analyse any impairment in the quality of services provided by the system
- Loss of data or of data integrity
- Failure in defining penalties within the contract
- Inconsistent application of contractual penalties provided in case of failure to meet the service level agreements
- Delayed management of expiry dates of the contracts
- Unauthorized changes to the data.

The introduction of any form of technology into a given production process, or merely the modification of an existing IT environment, requires extensive adaptation (in terms of staff skills, workflows, policies and procedures, etc.), which will dramatically change the risk profile of a department or process. Therefore, IT risks cannot be considered separately from other risks, such as people risk, process risk and others: recognizing these challenges and categorizing them under "IT-related risks" provide management with a stronger control of these risks (Fheili 2011).

The monitoring of operational IT risk across the numerous organizations becomes an important element of systemic risk management for the economy, and is reflected in the inclusion of IT risk guidelines in recent regulatory mandates, industry standards and enterprise risk management methodologies (Friedhoff and Mansouri 2015). BCBS (2014) underlines that a large number of banks have designed their IT policies

in order to fit local and international standards for IT controls. Among these, BCBS cites the following:

- Control Objectives for Information and related Technology (COBIT): an IT governance framework, developed by ISACA (previously known as the Information Systems Audit and Control Association), which aims primarily at compliance and security and, as such, provides globally accepted principles, practices, analytical tools and models for the governance and management of enterprise IT;
- Information Technology Infrastructure Library (ITIL): describes a systematic, professional procedure for the management of IT services focusing on the end user rather than on the technology.

4.6.2 IT as a Mitigation Factor

The areas of technological applications in OR management cover a very broad range embracing, for example, all the tools for decentralized data processing, centralized data analysis, report preparation, information collection and transmission, information storage and update. In addition to these examples of primary employment of software and hardware applications, there is also a range of solutions proposed for ensuring business continuity (in which the technological component has a strong role), and thus the development of plans for restoring functionality of the bank's vital processes and recovering physical or electronic documentary supports needed for the continuation of the activity.

Therefore, the framework of measurement and management of OR includes several key components of the information system: risk event monitoring procedures, databases for business processes and associated risk factors, monitoring systems and management reporting systems. The operational risk management requires, therefore, the availability of an IT equipment capable of handling, in an integrated and systematic way, OR management phases (identification, evaluation, monitoring, control, mitigation) in respect of the regulatory, organizational and methodological issues (Giardina and Ierardi 2009).

Therefore, banks must have an IT system capable of responding to the requirements established for OR management. The need for changes in bank applications and processes is obvious, and it is reasonable to think that this need is in conflict with the relatively rigid structure of the IT systems that the banks currently possess (Flores et al. 2006). The establishment of an OR Information System (IS) involves the need to remodel the bank's current IT-IS (in particular, the computerized accounting subsystem). Therefore, it is necessary that banks carry out remarkable IT investments, associated with a thorough redesign and/or restructuring of the organization so that the investments can bring benefits (Dos Santos and Sussman 2000).

In particular, in the AMA, information technology is relevant for implementing the procedures for the inclusion of internal operational losses in the database, for activating a data quality process (see Chap. 3) aimed at monitoring the quality of the loss data detection/collection, and for implementing specific software to support the management of insurance policies for the purpose of mitigating operational risks. The development of this software allows to collect within a single repository all the information related to the occurrence of loss events (e.g. thefts and robberies, ATMs burglaries, ATM fraud, damage to immovable assets caused by natural disasters/vandalism, damage to movable assets such as company cars and ATM equipment, embezzlement on behalf of employees), to the request for insurance recovery and the management of relations with insurance companies. This allows to reduce times of data collection needed for the management of insurance policies, to increase the quality of the information related to the operational loss events and the insurance recoveries and, finally, to perform better the analysis of pricing of insurance policies in force.

4.6.3 The Role of Internal Audit

In the case an external company providing IT services takes part in the management of a bank's OR, it is possible to pinpoint specific tasks to both the bank's IT internal audit and to the IA of the external service provider. The former is responsible for strengthening controls defined

within the IT processes, mitigating IT risks, managing the technological components, which need to be aligned with the objectives and strategies of the bank served by the external company. The IT auditors' role is particularly important towards:

- achieving the effectiveness and efficiency objectives defined for the services outsourced to the external provider;
- ensuring compliance with the requirements of quality and security of the information managed by the information systems;
- promoting a balanced control environment for the management of operational risk;
- guarding against the risks coming from the information systems.

In turn, the verification activities carried out by the internal audit of the external company are mainly directed towards (Giardina and Ierardi 2009):

- the OR management process, with an emphasis on the activities of internal loss data collection which represent the main information component used to define a reliable and accurate system for measuring operational risk;
- the reporting system on the operational risk management process, in order to ascertain:
  - the ability to provide the bank's supervisory and control bodies with all the data necessary and relevant to each stage of the OR management process (in terms of correctness and completeness);
  - the consistency of the information with the actual operational risk profile of the company, which can be compared with the risk appetite defined by the bank;
  - the timeliness of information, in relation to the ability to provide the management with the information necessary to a proper business management.

In such setting, it is also likely to hypothesize a joint activity of the IT auditor and the security officer.

While the IT auditor oversees the internal control system as a whole, the security officer is dedicated to the protection of corporate strategic assets and aims, in particular, to guarantee business continuity, in order to reduce interruptions of services and create value for the enterprise.

These roles are therefore able to enhance the components of the OR management process through:

- the identification and mapping of threats and vulnerabilities,
- the identification of new methods of risk analysis and assessment,
- the definition of specific monitoring activities concerning critical business areas,
- the determination of priorities in the planned measures for risk mitigation.

This joint intervention does not affect the independence of the internal audit and allows a continuous value creation in a context increasingly called upon to face complex challenges linked both to the rapid spreading of new interrelated threats (pharming, phishing, skimming, boxing, trashing, sniffing, vishing, organized crime, etc.) and to the increasing issuing of laws and regulations to comply with.

4.7 Conclusions

The board of directors and senior management should establish a corporate culture (Kaminski et al. 2016; EY 2015) that is guided by a strong risk management and that supports and provides appropriate standards and incentives for professional and responsible behaviour. In this regard, it is the responsibility of the board of directors to ensure that a strong operational risk management culture exists throughout the whole organization. On this basis, banks are asked to develop, implement and maintain a framework that is fully integrated into the bank's risk management processes. The framework for operational risk management chosen by a bank will depend on a range of factors, including its nature, size, complexity and risk profile.

Common industry practice for sound operational risk governance often relies on different lines of defence: one of these is an independent operational risk management function that should be fully integrated into the bank's overall risk management governance structure. This function may take care of the operational risk measurement and reporting processes. A key activity is to challenge the business lines' inputs to, and outputs from, the bank's risk management, risk measurement and reporting systems. The operational risk management should have a sufficient number of personnel skilled in the management of operational risk to effectively address its many responsibilities.

Notes

1. The sub-process is the set of activities that belong within a same process and which are linked to one another; the phase is defined as the range of functional activities towards the execution of a subprocess; lastly, the activity is defined as the set of connected actions and performed according to a logic and chronological sequence, usually without interruption.
2. OR culture is a combined set of individual and corporate values, attitudes, competences and behaviour that determine a company's commitment to and style of OR management. In particular, OR culture includes: (1) Integrity and ethical values; (2) Management philosophy and operating style; (3) Organizational structure; (4) Delegation of authority and responsibility; (5) Human Resources policies and practices; (6) Staff competencies (Prokopenko and Bondarenko 2012).
3. The first line of defence is business line management: it is responsible for identifying and managing the risks inherent in the products, activities, processes and systems for which it is accountable. Besides, the second line of defence is the corporate operational risk function: the responsibilities of this function include challenging the business unit inputs to, and the outputs from, the bank's operational risk management tools, operational risk measurement activities and operational risk reporting systems.
4. The management body is defined in point (7) of Article 3(1) of Directive 2013/36/EU: 'management body' means an institution's body

or bodies, which are appointed in accordance with national law, which are empowered to set the strategy, objectives and overall direction, and which oversee and monitor management decision-making, and include the persons who effectively direct the business of the institution.

5. Senior management is defined in point (9) of Article 3(1) of Directive 2013/36/EU: 'senior management' means those natural persons who exercise executive functions within an institution and who are responsible, and accountable to the management body, for the day-to-day management of the institution.
6. Operational risk tolerance is defined in EBA (2015), Article 8(1), point (b) (i), as "the institution's forward looking view of the aggregate level and types of operational risk that the institution is willing or prepared to incur which will not jeopardise its strategic objectives and business plan".
7. Operational risk tolerance statement is defined in EBA (2015), Article 8(1), point (b) (ii), as "the institution's written statement on the aggregate level of operational risk loss and event types—containing both qualitative and quantitative measures, such as thresholds and limits based on operational risk loss metrics—that the institution is willing or prepared to incur in order to achieve its strategic objectives and business plan".
8. The management and monitoring of the customers' claims often involve other functions, especially internal audit and compliance.
9. In this respect, Directive 2013/36/EU, Article 85(2), establishes that: "Competent authorities shall ensure that contingency and business continuity plans are in place to ensure an institution's ability to operate on an ongoing basis and limit losses in the event of severe business disruption."
10. The reference is to business environment and internal control factors (BEICFs).
11. As we have seen in Chapter 2, the EBA moves in the same direction: the compliance risk should fall within the OR. EBA makes it clear that this risk must be included in the definition of operational risk found in Article 4(1)(52) of Regulation (EU) No. 575/2013 (CRR): it is one of the many different categories of operational risk.
12. Many banks produce quarterly operational risk reports, but only a few banks produce them on a monthly basis.

References

Bazzarello, D., and D. Maucci. 2009. Le funzioni aziendali e i RO: l'esperienza UniCredit. In *Il Rischio operativo nelle banche italiane. Modelli, gestione e disclosure*, ed. G. Birindelli and P. Ferretti. Roma: Bancaria Editrice.

BCBS-Basel Committee on Banking Supervision. 2005. Compliance and the compliance function in banks, April.

BCBS-Basel Committee on Banking Supervision. 2013. Principles for effective risk data aggregation and risk reporting, January.

BCBS-Basel Committee on Banking Supervision. 2014. Review of the principles for the sound management of operational risk, October 6.

Berlanda, M. 2009. La collaborazione con la funzione Risk Management. Paper presented at Associazione Bancaria Italiana Convention on Compliance in Banks, Dalle regole alle strategie di business, Milano, 20–21 ottobre.

Birindelli, G., and P. Ferretti. 2008. Compliance risk in Italian banks: The results of a survey. *Journal of Financial Regulation and Compliance* 16 (4): 335–351.

Birindelli, G., and P. Ferretti. 2009. *Il presidio organizzativo del RO e gli strumenti di mitigazione. In Il Rischio operativo nelle banche italiane. Modelli, gestione e disclosure*, ed. G. Birindelli and P. Ferretti. Roma: Bancaria Editrice.

Birindelli, G., and P. Ferretti. 2013. Compliance function in Italian banks: Organizational issues. *Journal of Financial Regulation and Compliance* 21 (3): 217–240.

Brienza, P., and P. Gianturco. 2005. I profili organizzativi della struttura di Operational Risk Management. In *Il rischio operativo nelle banche*, ed. G. Gabbi, M. Marsella, and M. Massacesi. Milano: Egea.

Cagan, P. 2006. On finding linkages: Corporate governance and operational risk. *The John Liner Review* 19: 7.

Dos Santos, B., and L. Sussman. 2000. Improving the return on IT investment: The productivity paradox. *International Journal of Information Management* 20: 429–440.

EY. 2015. Rethinking risk management.

Fernández-Laviada, A. 2007. Internal audit function role in operational risk management. *Journal of Financial Regulation and Compliance* 15 (2): 143–155.

Fheili, M.I. 2011. Information technology at the forefront of operational risk: Banks are at a greater risk. *Journal of Operational Risk* 6 (2): 47–67.

Flores, F., E. Bónson-Ponte, and T. Escobar-Rodríguez. 2006. Operational risk information system: A challenge for the banking sector. *Journal of Financial Regulation and Compliance* 14 (4): 383–401.

Friedhoff, J., and M. Mansouri. 2015. Monitoring IT operational risks across US capital markets. *Journal of Operational Risk* 10 (2): 61–97.

Garnero, R. 2003. Audit Management: una metodologia di valutazione dei rischi aziendali. In *I controlli interni nelle banche. Evoluzione, metodi e casi pratici*, ed. M. Alonzo, A. Chiarotto, R. Garnero, C. Giaj Levra, S. Panebianco, A. Pappadà, and G. Varola. Roma: Edibank.

Giardina, V., A. Ierardi. 2009. La governance del framework ORM e la sana e prudente gestione dell'Information Technology: l'esperienza del Consorzio Operativo Gruppo Montepaschi. In *Il Rischio operativo nelle banche italiane. Modelli, gestione e disclosure*, ed. G. Birindelli, and P. Ferretti. Roma: Bancaria Editrice.

Gusmeroli, M., A. Bonolo. 2009. Il RO e la revisione dei processi aziendali. In *Il Rischio operativo nelle banche italiane. Modelli, gestione e disclosure*, ed. G. Birindelli, and P. Ferretti. Roma: Bancaria Editrice.

Kaminski, P., D. Mikkelsen, T. Poppensieker, and A. Raufuβ. 2016. Nonfinancial risk: A growing challenge for the bank, McKinsey, July.

Lyons, S. 2006. Corporate defence: Are stakeholders interests adequately defended? *Journal of Operational Risk* 1 (2): 63–73.

Metelli, F. 2005. Dalla teoria alla pratica: la strada dell'operational risk management in una banca italiana, Corso di aggiornamento A.S.S.B.B. – Università Cattolica su Il Rischio Operativo nelle Banche: Metodologie di valutazione e strumenti di copertura assicurativa, Milano, 7–8 Giugno.

Milkau, U. 2013. Adequate communication about operational risk in the business line. *Journal of Operational risk* 8 (1): 35–57.

Miranda, A. 2000. Rischio operativo e intermediazione finanziaria, *Bancaria* 7–8.

Paessler, D. 2014. Visibility in IT operational risk management. The role of network, White Paper, June.

Pandey, D. 2008. Who 'owns' operational risk? http://ssrn.com/abstract=1262606.

Pasquini, C. 2009. Introduzione alla sessione 'Modelli e fattori di successo: esperienze a confronto'. Paper presented at Associazione Bancaria Italiana Conference on Compliance in Banks, Dalle regole alle strategie di business, Milano, 20 e 21 ottobre.

Prokopenko, Y., and D. Bondarenko. 2012. Operational risk management: Best practice overview and implementation, Risk professional workshop, Tirana, Albania, September 10–11.

Renna, S. 2007. La gestione del rischio legale: ruoli ed interazioni fra le funzioni di ORM e di Compliance. In *Basilea 2. Cosa devono fare le banche adesso. Le nuove disposizioni di vigilanza e i processi implementativi in atto, Atti del convegno del 22 e 23 gennaio*, ed. ABI – Associazione Bancaria Italiana, 67–80. Roma: Bancaria Editrice.

Scoppio, M. 2005. Punti di attenzione nel quadro regolamentare: internal auditing, sound practice, operational risk e "nuova" funzione di compliance, Intervento al Seminario ABIFORMAZIONE su Lineamenti evolutivi della funzione di Internal Audit, Milano, 24–25 febbraio.

5

Operational Risk Mitigation: Strategies and Tools

5.1 Introduction

Banks adopting advanced measurement approach have the possibility of reducing the operational risk capital requirement in presence of insurance and other risk transfer mechanisms as they demonstrate that a noticeable risk-mitigating effect is achieved and the mitigation techniques comply with specific standards.

In this chapter we describe the regulatory framework of the operational risk mitigation techniques and we analyse, particularly for insurance, the main operational issues of their use as operational risk mitigants, highlighting the most relevant impacts on the banks' operational risk management. We also describe the most widespread instruments banks may use: both traditional and innovative ones.

G. Birindelli and P. Ferretti, *Operational Risk Management in Banks*,
Palgrave Macmillan Studies in Banking and Financial Institutions,
DOI 10.1057/978-1-137-59452-5_5

5.2 Recognition of OR Mitigation Techniques: The Regulatory Framework

The regulatory framework allows banks adopting AMA methodology the possibility of reducing the operational risk capital requirement in presence of insurance and other risk transfer mechanisms—ORTMs (see Chap. 3)—inasmuch as the bank demonstrates that a noticeable risk-mitigating effect is achieved and the mitigation techniques comply with specific standards (Article 323—CRR 575/2013; EBA 2015).

In particular, when the mitigation techniques are in the form of insurance (among others, Kuritzkes and Scott 2005), the provider must be authorized to provide insurance or reinsurance—either in the EU or in jurisdictions with equivalent regulatory standards for insurance companies. Furthermore, the provider must have a minimum claim-paying ability rating warranted by an eligible credit assessment institution (ECAI), which the EBA has established to be associated with credit quality step 3 or above under the rules for risk weighting of exposures to corporate under the standardized approach for credit risk.

In order to prevent circumvention of rules, the insurance must meet specific conditions. It must be provided via a third party, and multiple counting of techniques must be avoided. Accordingly, it is necessary to ensure that neither the institution nor any of the entities included in the scope of the consolidation has a participation or a qualifying holding in the party providing the insurance and is knowingly reinsuring contracts covering OR events that form the object of the initial insurance arrangement entered by the institution.

Appropriate risk mitigation calculations should also reflect the insurance coverage and the framework for recognizing the need of insurance being sturdy and well documented. In particular, insurance coverage should be aligned with the institution's risk profile and comply with the likelihood and impact of all OR losses (insurance risk mapping process). Also, the institution should estimate the likelihood of insurance recovery and the possible time frame for the receipt of payment by insurers (for example, likelihood of a claim being litigated, the length of the process and current settlement rates and terms), based on the experience of

the insurance risk management team and supported, where necessary, by appropriate external expertise (e.g. claims counsel, brokers and carriers; BCBS 2010; EBA 2015). The institution should assess the performance of insurance in the event of an OR loss based on previous estimates and should design such process, so that it is able to assess the insurance response for any relevant loss and data-scenario entered into the capital model. The institution should then painstakingly map the insurance policies based on previous assessments regarding the institution's risks, using all the information sources available, such as internal data, external data and scenario estimates. The institution must also conduct the mapping with transparency and consistency, and assign the appropriate weight to past and expected insurance performance through the appraisal of each insurance policy component. Lastly, the institution must obtain formal approval from the appropriate risk body or committee, and periodically re-examine the insurance mapping process.

The framework for recognizing insurance also foresees the use of a sophisticated risk mitigation calculation. In such case the modelling approach for incorporating the insurance coverage within the AMA must be consistent with the OR measurement system adopted to quantify the gross-of-insurance losses, be transparent in its relationship with the effective likelihood and impact of losses used in the institution's overall determination of AMA's fund requirements and consistent with that relationship.

Lastly, the risk mitigation calculation needs to be aligned to the OR profile in a timely fashion. Therefore, whenever the nature of the insurance changes significantly or a major change occurs in the institution's OR profile, the institution must review the use of insurance and recalculate the AMA capital requirements. In the event material losses affecting insurance coverage occur, the recalculation of the AMA capital requirements should consider an additional margin of conservatism. Whenever an unexpected termination or reduction of the insurance coverage occurs, the institution must be prepared to promptly replace the insurance policy on equivalent or improved terms, conditions and coverage or to increase the AMA capital requirements to a gross-of-insurance level. Finally, the institution must calculate capital on a gross and net-of-insurance, at a level of granularity such that any erosion in

the amount of insurance available (e.g. payment of a material loss) or a change in insurance coverage can be immediately recognized for its effect on the AMA capital requirements (EBA 2015).

A further issue concerns the suitability of the methodology for recognizing insurance to capture all the relevant elements through discounts or haircuts in the amount of insurance recognition. Specifically, the institution should investigate any factors that may prevent the insurance from issuing the coverage expected and hence decrease the effectiveness of risk transfer (payment uncertainty) as well as any critical issues preventing the ability of the institution to identify, analyse and report the claim as expected. To this end, it is also important to verify how the mentioned factors have affected the mitigating impact of insurance on the OR profile in the past and how they might affect it in the future. Payment and the other aforesaid uncertainties must be reflected in the AMA capital requirements through appropriately conservative haircuts. Moreover, the institution should take into account the characteristics of the insurance policies: e.g. whether they exclusively cover losses claimed or notified to the insurer during the term; whether they cover losses incurred during the policy term, even where they are not discovered and the claim is not lodged until after expiration of the policy; whether the losses are first-party direct losses or third-party liability losses. The institution must document data on insurance pay-outs by loss type and set haircuts accordingly.

In the attempt of verifying the true coverage protection provided by the insurer or the ability to receive the claim payment funds within a reasonable time frame, the institution should set in place procedures for loss identification, analysis and claims processing. The institution must quantify and model haircuts separately for each of the identified relevant uncertainties. However, no single haircut can be applied in the calculation of all uncertainties, nor an ex-post calculation haircut can be made. The institution must take into account the insurer's risk of claim-paying ability, by applying appropriate haircuts in the insurance modelling methodology. Moreover, it should ensure that the claim-paying ability risk for counterparty default is assessed on the basis of the credit quality of the insurance company responsible under the given insurance contract, independently of whether the insurance company's

parent institution has a better rating or whether the risk is transferred to a third party. Conservative assumptions should be made about the renewal of insurance policies in terms of equivalent conditions and coverage as the original or existing contracts. The institution should have processes in place to guarantee that the potential exhaustion of insurance policy limits, the price and availability of reinstatements of cover, and coverage mismatches (cases in which the coverage of the insurance contract does not match the OR profile) are reflected in the AMA capital requirements. The requirement of applying haircuts for the residual term (period before expiry of the insurance contract) or for the cancellation term can be waived if (a) the institution can demonstrate the existence of continuous coverage on equivalent or improved terms (for at least 365 days) or (b) it has an insurance policy that cannot be withdrawn by the insurer or that has a cancellation period of over 1 year.

5.2.1 Brief Considerations on Other Risk Transfer Mechanisms

If the mitigation techniques are in the form of ORTMs rather than insurance, the institution must demonstrate that they are truly transferring risk and these tools are not used to elude AMA capital requirements. In light of the peculiar features of OR—where there are no clear underlying assets of reference and where unexpected losses play a greater role than in other types of risks—this is a pivotal aspect. This condition is further exacerbated in the light of the lack of an efficient, liquid and structured market for OR products which have so far been traded outside the banking sector (catastrophe bonds, weather derivatives, etc.). Often assessing the legal risk of such mechanisms is difficult, even when the terms and conditions are clearly and carefully spelt out. In order to ensure that a noticeable risk-mitigating effect is achieved with the use of ORTMs, the institution should demonstrate experience in using them, and define their characteristics (e.g. probability of coverage, timeliness of payment) before they be recognized in the OR measurement system. ORTMs are not accepted as eligible risk mitigation tools of the AMA capital requirements when they are held or used

for trading purposes, rather than for risk management purposes. The ORTM is subject to verification in terms of eligibility of the protection seller (e.g. regulated or unregulated entity) and the nature and characteristics of the protection (e.g. funded protection, securitization, guarantee mechanism, derivatives, etc.). The institution must calculate the AMA capital requirements on a gross and net of ORTMs basis for each capital calculation. The level of granularity needs to be such that an erosion in the amount of protection available can be immediately recognized in terms of its impact on capital requirements. When material losses affect the coverage provided by the ORTMs, or when changes in the contracts create major uncertainty in terms of coverage, the institution must recalculate its capital requirements with an additional margin of conservatism.

In closing, we shall recall that the reduction in capital requirements from the recognition of insurances and ORTMs cannot exceed 20% of the own funds requirement for OR prior to the recognition of risk mitigation techniques, and that a bank using AMA for the calculation of its OR capital requirement must disclose a description of the use of insurance and ORTSs for OR mitigation.

5.3 Mitigation Policies: Some Operational Issues

The option of AMA banks employing insurance tools to reduce OR capital requirement has brought a renewed interest of the financial community towards the opportunities linked to the use of insurance coverage. Indeed, despite insurance policies having always represented one of the methods for managing operational risks, their potential within the OR processes has become more evident with the introduction of the regulatory provision on OR mitigation. Such aspect has thus compelled intermediaries to review the evaluation procedures of insurance products (which in most cases are based on their costs and on budget available rather than on the risks they should cover) and to gain better understanding on the most convenient ways to match insurance

demand-and-supply, in order to be less susceptible to the influence of insurance brokers.

Operational risk management procedures depend on many factors, including the bank's risk appetite, its capacity of risk retention, and its tolerance towards the volatility of cash flows (KPMG 2008). On broader terms, the management approaches of pure risks (to which OR refers) are distinguished into control and financing techniques.

The first category (control approaches) foresees preventive actions towards reducing the probability of occurrence of prejudicial events, as well as protective actions towards limiting the damage arising from such events. The control approach also includes physical control techniques, among which (i) the use of measures able to limit the likelihood of a risk event or of related losses, (ii) procedural techniques, consisting in the provision of rules of conduct; and, finally, (iii) psychological techniques, designed to promote a risk culture within the bank.

The second category (financing approaches) foresees intervention on the economic-financial impact determined by the adverse event. Such methods may be either implemented as risk transfer—typical of the insurance phenomenon—or as risk retention, for which financial planning is pivotal in consideration of the need to create financial resources within the bank that can cover the costs arising from the occurrence of the risk event.

Hence, in keeping with the general considerations of a unitary logic of risk management, an appropriate OR control system shall be based on different solutions, whose characteristics allow to match a specific option to each specific type of operational risk. In other words, by distinguishing the operational risks in terms of frequency and severity, it is possible to establish a correlation between classes of risk and type of management approaches (Sironi 2003; Locatelli 2001). Although the decision of replacing a specific management approach in favour of another is based on criteria of economic convenience and effective protection, in the case of high-frequency, low-impact (HFLI) events—and even more of low-frequency, low-impact (LFLI) events—it is likely that the most appropriate choice be that of retention, which can be achieved through allocations to reserve for covering the expected loss and own funds for covering the unexpected one. In the event the intermediary's

capacity of risk taking is not compatible with the peculiarities of the risk event, alternative solutions are represented by hedging tools or—considering the scarce diffusion of such latter solution for ORs—by measures able to minimize the probability of occurrence, or by resorting to insurance policies. The latter, however, are unsuitable for facing high-frequency, high-impact (HFHI) events, typically internal events, for which measures such as strengthening of human capital, of control procedures, and of information systems are more appropriate. Lastly, as to low-frequency, high-impact (LFHI) events, some opportunities may derive from the transfer of activities (outsourcing) or of financial impact. In the former case (outsourcing) it is essential that the responsibilities between the parties be shared, keeping in mind that performing the external functions safely and correctly remains responsibility of the board of directors and top management. Equally important is the management of residual risks associated with the possibility of dysfunctions in the provision of services. In the second case, reference is made to insurance coverage (Blacker 2000; Peters et al. 2011; Bazzarello et al. 2006), whose mitigating efficacy is correlated to the characteristics of the type of risk we are being dealt with: low statistical frequency, potential of a heavy financial impact, difficult control on the part of the exposed subject, and external origin. The insurance tool gains even further value if we consider the difficulty of VaR models in detecting low-frequency events (Sironi and Resti 2008). In reference to this last point, it is worth underlining that not all LFHI events are manageable through the insurance tool, either because of the low level of development of the insurance (as for example in the case of catastrophic events) or because of the excessive burden on the policy holder, in which cases banks can decide to take action exclusively on the internal control systems. Finally, it is necessary to check that the abatement of OR derived from the use of insurance does not imply transfer of risks to other sectors or the creation of new ones.

In any case, among the reasons for which the intermediary turns to the insurance tools, noteworthy is the impact on the distribution of losses (Scott and Jackson 2002). In the presence of an insurance coverage, the standard deviation of the single events—associated with unexpected losses—tends to diminish, insofar as the premiums paid by the

bank are predetermined (Fig. 5.1). In principle, the price of insurance coverage should coincide with the expected value of the loss during the period of validity of the policy, increased by remuneration for the insurance company, which could however increase excessively the cost of the policy. This explains why the value is greater than average, in comparison with the hypothesis of non-insurance of the risks. In such case the decision of the bank to support a higher cost for the expected value of the loss depends on the uncertainty of the assessment.

However, it is also true that the insurance company may limit the costs, through the diversification policies and pooling of risks, which determine a reduction in both the standard deviation and the average. The possibility for the insurance company to achieve economies of scale allows setting more admissible pricing policies for banks. This is particularly true for low-frequency events—although not for those with very low likelihood (such as catastrophic events for which the insurance instrument does not represent the optimal solution, and which require a wide availability of data to be appropriately measured).

Another advantage connected with the use of the insurance coverage is represented by the opportunity to free capital that would otherwise be allocated to covering OR, making it available for profitable

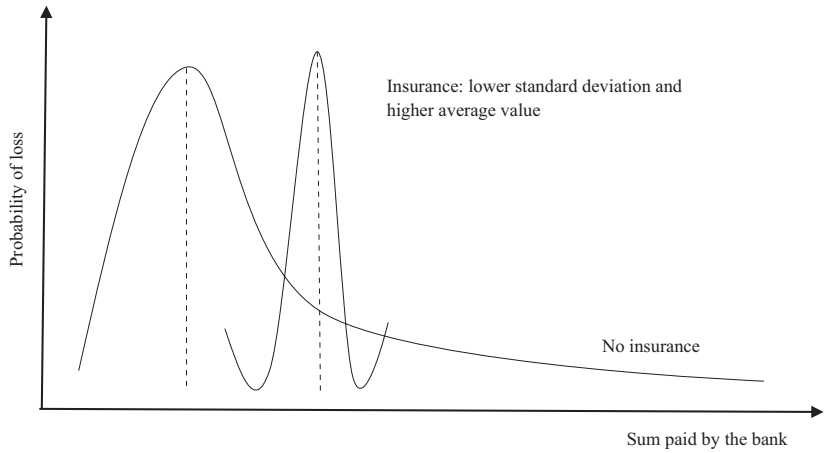


Fig. 5.1 Insurance impact on the Loss distribution curve (Scott and Jackson 2002)

opportunities of investments. Moreover, the use of insurance allows finding capital resources in circumstances in which funding tends to diminish, as in the case ORs arise. On the other hand, the OR transfer exposes the bank to the risk of the insurer's default (Li et al. 2011)—unlikely, especially in the presence of high rating, yet possible—at the occurrence of the adverse event. Moreover, the insurance company could fulfil its obligation, but delay the times of payment, with foreseeable inconveniences for the bank in terms of timely availability of funds.

If on one hand the integrated risks management allows insurance companies to exploit specialization advantages and to achieve cost-savings that can favour more convenient pricing policies, on the other hand, the specificity of ORs to which banks are exposed amplifies the information asymmetries between them and the insurance companies, who are hence unable to evaluate conveniently the counterpart's actual risk. The effect of moral hazard, however, can be circumscribed by including dedicated clauses in the insurance contract—first and foremost the deductible. The fact that a part of the risk remains upon the bank should encourage it to improve its own risk management.

Owing to the regulatory provision on mitigating ORs through insurance coverage, in respect of precise criteria referring both to the policies and to the insurance companies, many critical elements hinder the full implementation on behalf of banks.

Among these is the less than satisfactory matching between insurance coverage and event types defined by the supervisory authorities, which undermines the ability of the insurance policies to face the different OR types, as is seen especially in some financial systems like the Italian one. Just as frequent is the situation in which risk events are covered by multiple policies (often deficient in terms of harmonization), while other events are only scarcely covered (Franzoso 2005).

The need to improve the convergence between insurance offer and banks' needs requires that banks map risks to be insured (insurance mapping) in order to understand whether insurance products match operational losses or not. To such purpose, it is fundamental that there be a more dialectic relationship between the organizational unit assigned to the management of insurance policies and ORM (Lemmi Gigli 2005) since the results of the process of ORs identification and

evaluation should support decision-making in the field of insurance, particularly in reference to the definition of policies requirements. In reference to this, it is important to consider the suitability of the loss distribution approach (see Chap. 6) for evaluating the impact of insurance solutions on OR exposure and thus their level of efficacy and effectiveness; such approach also allows identifying the pure component of the premium (Vellella 2005).

From the insurance market's perspective, there are several critical factors to be considered. In principle, such factors can still be traced to the fragmented nature of the insurance industry, to the limited diversification of products, to the widespread technical complexity of the wording of the insurance contracts, to the scarce transparency of the pricing and to the heavy deductibles and premiums paid by the banks. It may be necessary to remodel the insurance offer through a comparison with banks, in order to understand their specific needs and the ability to evaluate their OR exposure (Marzano 2005). Accordingly, banks need to enhance their communication skills in portraying the operational risk as well as their risk management policies, in a way that these can be conveniently assessed by the insurance industry and in turn be expressed in the policies under the form of more favourable contract terms, such as reduced deductibles and/or premiums.

Criticisms have also been advanced with respect to the decision of the supervisory authorities to limit the AMA bank's use of the insurances as factors of OR mitigation, denouncing the distorting effect on the competitiveness of the banking system. Indeed, an effective risk transfer strategy can benefit the management of all the intermediaries, including those adopting the most simplified methods (SA and BIA), which are numerically significant. On the other hand, it is likely that only the large-sized intermediaries and those with more sophisticated risk management policies—presumably those adopting advanced methods—are able to evaluate the insurance tool more effectively, to support the high costs of the policies and to control better the volatility of cash flows related to a possible payment default or delay by the insurance company.

The dreaded competitive disadvantage to the detriment of smaller institutions is somewhat weakened by the limited use of insurance tools

by the banking industry, as confirmed by the results of the Loss Data Collection Exercise (LDCE), conducted in 2008 on 121 intermediaries (42 AMA banks and 79 non-AMA banks) from Australia (11 banks), Europe (60 banks), Japan (18 banks), North America (23 banks), Brazil/India (9 banks) (BCBS 2009). The LDCE collected qualitative information, exposure indicators, capital estimates, and a wide range of practical information as to how OR is measured and managed. Given the broad participation in this exercise (the previous exercise is dated 2002), the results can be viewed as generally representative of the banking industry.

With reference to insurance recoveries, the banks were asked to provide the total amount of insurance recoveries associated with each loss in their internal data submission as well as an indication of whether the loss was covered by an insurance policy. As a number of banks had some difficulties in mapping insurance coverage to individual loss events, there was some uncertainty arising from the insurance coverage indicator; given this uncertainty, the analysis included data from participating institutions that had reported insurance recovery information for at least one loss. The key findings are shown in Tables 5.1 and 5.2.

Table 5.1 reports the number of losses with insurance recoveries as a percentage of the total number of losses, the total amount of insurance recoveries divided by the total amount of losses with an insurance recovery (loss amounts refer to gross loss net of all non-insurance recoveries), and the total amount of insurance recoveries divided by the total value of all losses (loss amounts refer to gross loss net of all non-insurance recoveries). These three ratios were estimated both for all-size losses and

Table 5.1 Insurance recoveries (BCBS 2009)

All banks	Percent of losses with an insurance recovery (%)	Recovery rate for losses with recoveries (%)	Amount recovered as a percent of total loss amount (%)
All losses	2.1	74.6	3.1
Median (25–75th)	(0.4–8.3)	(59.3–89.9)	(1.3–9.5)
Losses $\geq$ € 20,000	4.2	70.5	3.0
Median (25–75th)	(1.3–15.6)	(53.2–87.1)	(0.7–11.8)

Table 5.2 Insurance recoveries by event type (BCBS 2009)

All banks	Percent of losses with an insurance recovery (%)	Recovery rate for losses with recoveries (%)	Amount recovered as a percent of total loss amount (%)
Internal fraud	0.00	62.94	0.00
Median (25–75th)	(0.00–3.37)	(36.36–79.58)	(0.00–2.00)
External fraud	8.84	77.91	7.17
Median (25–75th)	(0.43–33.50)	(58.30–96.21)	(58.30–96.21)
Employment practices and workplace safety	0.00	91.32	0.00
Median (25–75th)	(0.00–0.30)	(44.14–100.00)	(0.00–0.35)
Clients, products and business practices	0.00	67.73	0.00
Median (25–75th)	(0.00–0.07)	(31.40–85.41)	(0.00–0.03)
Damage to physical assets	27.91	81.28	19.83
Median (25–75th)	(0.00–57.69)	(67.00–93.20)	(0.30–51.35)
Business disruption and system failures	0.00	85.35	0.00
Median (25–75th)	(0.00–0.00)	(61.54–95.73)	(0.00–0.17)
Execution, delivery and process management	0.00	71.64	0.01
Median (25–75th)	(0.00–0.80)	(45.70–92.27)	(0.00–0.33)

for losses over € 20,000. Median 25–75th represents the interquartile range, which is the range of values (between the 25 and 75th percentile) including 50% of the banks in the sample.

Only a small proportion of the losses had an associated insurance recovery. The values indicate that 2.1% of all losses and 4.2% of losses of € 20,000 or more were offset to some degree by an insurance recovery (the results for insurance recoveries in the previous loss data collection exercise, 2002 LDCE, were similar). The median recovery rate was 74.6% for all losses and 70.5% for losses of € 20,000 or more, indicating that for losses with insurance recoveries at least half of the banks had a significant portion of the loss amount offset by insurance. Finally, a small percentage (approximately 3.0%) of the total amount of internal losses was recovered through insurance.

By distinguishing AMA and non-AMA banks, it should be underlined that the former had a much lower ratio of losses with recoveries compared to the others, but reported similar recovery rates. The lower ratio of losses with recoveries may reflect the nature of losses at AMA banks, since they may be more likely than non-AMA to experience larger, non-insurable events.

Table 5.2 shows insurance recovery patterns across event types for losses of € 20,000 or more. Insurance recoveries were most commonly mapped to losses classified as Damage to Physical Assets. A typical bank had 27.9% of the Damage to Physical Asset losses associated with an insurance recovery. This is not surprising as property insurance is a standard insurance policy purchased by banks. External Fraud losses had the second highest median ratio of losses with insurance recoveries (8.84%). For all other event types, more than half of banks had no recoveries associated with their losses. Recovery rates ranged from 62.94% for Internal Fraud losses to 91.32% for Employment Practices and Workplace Safety losses. For the amount recovered as a percentage of the total loss amount, median ratios were zero in all event types except for Damage to Physical Assets with a ratio of 19.83%, External Fraud (7.17%) and Execution, Delivery and Process Management (0.01%).

5.4 Mitigation Tools: Traditional Versus More Innovative Instruments

Among the mechanisms of OR transfer, the insurance tool is certainly the most important. However, for some types of OR, recourse to the insurance market is not all that suitable, owing for example to the very low-likelihood, high-impact features of the risk event. Hence the search for a convergence between insurance and finance through the development of alternative risk transfer solutions (Alternative Risk Transfer—ART), characterized by a high degree of innovation in terms of mode, duration and hedging (Miani 2004).

5.4.1 Insurance Offer

Over the years the insurance offer has been enriched in response to the changing nature and types of ORs, to such an extent that the contracts covering events such as theft and robberies have been complemented by policies designed to face risks related to information technology, responsibility of the banks and of their employees towards clients, and responsibility of the managers towards the shareholders. The types of damages against which banks generally seek to protect themselves by means of insurance are material damages caused by external events and impoverishment for compensation to third parties arising from responsibilities associated with the activities performed. Policies of more or less ancient origins are taken out for these purposes. Among the more traditional policies, we may mention those covering accidents, health and fire; the latter aimed at safeguarding the physical assets of the bank, mainly against the occurrence of low-frequency, high-impact risks (risk of fire and natural events). The progressive relevance of Information Technology in the banking activity explains the increased importance of information policy in the current panorama of insurance products negotiated by intermediaries.

From a more operational standpoint it is possible to identify policies specifically designed for the financial sector, which are rather diffused internationally.

Among these, first of all, is the *Bankers Blanket Bond*, as an example of a "basket or umbrella" insurance product, i.e. the coverage of multiple risky events. This represents one of the most common policies adopted by the institutions involved in the provision of financial services to third parties (all financial institutions, investment managers and investment funds). It provides protection against the direct financial loss sustained as a result of various events, such as employee infidelity; the physical loss of property on premises and in transit; the forgery and alteration of monetary instruments and other documents of value; computer and cyber fraud as well as payments for fraudulent electronic funds. The coverage provided protects the balance sheet for fraud

against an organization and, especially for larger organizations, it further guarantees that funds and property are adequately safeguarded.

Another type of coverage is represented by the *Professional Indemnity Insurance*, which provides protection against legal liability to third parties. These liabilities can result from negligent acts, errors or omissions committed by the officers or employees of the organization. Claims may come from a variety of sources and jurisdictions which can include losses due to advice or negligence in carrying out professional duties.

Another policy is that of *Cash and Valuables in Premises and Transit*. This insurance provides coverage against the risks of physical loss or damage arising from whatever cause (e.g. theft, fire, theft by employees, mysterious or unexplained disappearance). Specific items covered include: cash and securities, gold and precious metals; safes, vault or tellers (at the insured person's premises); transits of cash/securities by banks using their own vehicles or staff; automated teller machines both on and off-site; customers' safety deposit boxes; brokers/dealers for investor compensation insurance. Typically, war- and terrorism-related incidents are not covered by this insurance; however, organizations can pay an additional premium to have these included in a policy. This type of coverage can work in conjunction with, or completely separately to, the Bankers Blanket Bond insurance and in many cases it offers an additional coverage that the Banker's Blanket Bond insurance does not (for example, cash inside customers' safety deposit boxes is covered here but not by the Bankers Blanket Bond). This policy is commonly requested by the financial institutions that have stocks of cash or valuables on their premises or in transit, or have a liability towards their customers for their customers' safety deposit boxes.

The insurance offer in favour of the financial institutions also includes the *Crime Insurance* policy. It is designed to protect the direct financial loss arising from any employee's fraud or from a dishonest act of a third party. Purchasing crime coverage should form part of a comprehensive risk management strategy that helps to offset the financial burden from such losses, and that demonstrates the management's awareness of a real threat.

There is also *Cyber Insurance*, which covers the losses related to damage to, or loss of, information from IT systems and networks. The

protections provided differ and include privacy protection: third party and employee privacy liability for damages and claims expenses resulting from privacy breach; privacy regulatory defence and penalties; reputational risk extension resulting from data breach. Another form is the cyber liability protection, which includes the security liability for damages and claims expenses that the insured person is legally obliged to pay, as it arises from computer attacks caused by failure in security; negligent transmission of a virus (damage to a customers' computer system and/or data); multimedia liability; intellectual property infringements. Other coverage is provided for data/electronic information loss (costs to restore data that has been lost or is corrupted); cyber extortion coverage (covers both the costs of investigation and the extortion demand amount related to a threat of a computer attack).

A specific policy, the *Directors and Officers Insurance* (D&O), safeguards the civil liability of the top management of the bank and aims at protecting the directors and key managers (officers) against claims by shareholders, investors, employees, regulators, etc., who have been negligent in the performance of their duties. Negligent acts include breach of trust, breach of duty, neglect, error, misleading statements, wrongful trading, etc.

A policy offering a coverage that goes beyond that of a standard D&O is *Employment Practices Liability*; it provides protection for the institution and all its employees (directors, officers and temporary workers). Such protection includes, among others, defence costs, mental anguish, emotional distress and regulatory investigations.

Finally, there is a type of insurance offering solutions to support the closing of Merger and Acquisitions (M&A) deals. In a challenging M&A climate, there has been a steady increase in the number of M&A deals where sellers are unwilling or unable to provide more than very basic warranties and indemnities. Escrow arrangements are often set in place to protect against unforeseen financial risks. However, escrows can be costly and have actually become less favourable in the current economic climate. An ideal alternative may be found in insurance solutions, which can offer a more cost-effective route in a wide range of transactions. For example, the buyer can arrange a policy to protect against any falsification or non-disclosure in relation to the warranties

and indemnities provided by the seller in forming the sale and purchase agreement. Sellers can arrange a policy to protect against claims by the buyer.

5.4.2 Alternative Risk Transfer Mechanisms

The ART solutions appeared in the 1970s for initiative of operators of the insurance industry and of the capital market, interested in exploiting potential synergies for the development of new opportunities for risk management. Although characterized by modest development, they pursue important purposes, such as the coverage of risks considered uninsurable, either for their large size and/or for very low frequency; reduction of the default risk of the insurance company; containment of premiums; possibility of avoiding the restricted offer in the traditional markets.

The classification of ART products distinguishes between risk transfer instruments via alternative operators (carriers) and, according to a more recent and broader meaning, the forms concentrated on risk financing.

Among the former, an important role is played by the captive companies (Tagliavini 1994; Mendolia 2001; Pisani 1996) which, in the form of insurance/reinsurance companies of the property of a company/group of companies not of an insurance nature, are set up to provide full or partial coverage for the risks assumed by the parent company. The creation of a captive company presents a number of advantages, especially in the medium-to-long term. Being under all aspects of an insurance/reinsurance company, a captive company represents a profit centre and an interesting opportunity to diversify business, with foreseeable benefits for the parent company. It is possible to reduce the total cost of risk management, as long as streamlining of the traditional insurance programmes is favoured, thanks to a greater bargaining power and to the concentration of insurance relations with a limited number of counterparties. Such positive aspects are yet associated with several issues. Firstly, the risk arising from the claims/premiums ratio, to which the captive is exposed, with the risk being more pronounced in the early years because of scarce financial strength that may be unable to absorb

unexpected losses. The choice of the location of the captive can be difficult, given that the differences in the financial and taxation systems can have a significant impact on the operating costs of the company. Finally, another issue may be a certain organizational complexity connected, among others, to the need to create a strong coordination among the different operational functions.

With regard to the risk financing techniques, first consideration should be given to the finite risk programmes, the peculiarity of which is to share a single risk over time. It is in function of this variable that they are qualified as prospective (a guarantee for claims that have not yet occurred) and retrospective (to cover claims that have already taken place but have not yet been paid). Further distinctive features are the multi-year duration (3–5 years), which allows levelling of the losses on a fairly long term, thus reducing the volatility of the results over the period, and the sharing of these by the contractor. The burden of the operation depends on the results obtained, in that when the loss ratio exceeds the prefixed capacity, the additional premiums must be paid. By contrast, in the case of premium surplus, they are repaid or capitalized for further coverage.

Multiline integrated multi-year products are also available, where a single contractual scheme—also in this case multi-year—includes a variety of risks: the possibility of bringing together unrelated risks produces the undeniable benefit of lowering the volatility of the share of the risk retained in the portfolio.

Over the years, coping with some of the OR types has also occurred by turning to derivative contracts, such as the operational risk swap and the first loss-to-happen put. In the latter case, for example, the protection buyers decide both on the events from which they intend to protect themselves and on the maximum loss limit; in the case of a single event and the exceeding of the threshold, the seller of the put covers the loss, whereas if the events are multiple, the damage is higher.

The catastrophic nature that the operational losses may assume explains the interest in the catastrophe bonds issued as part of securitization operations.

As a rule, the firm intending to transfer the risks (sponsoring firm) subscribes the entire capital in a Special Purpose Vehicle (SPV) from

which it receives reinsurance coverage by signing a contract—namely, a reinsurance contract—linked, in terms of duration, nature of risk, amount and type of guarantee, to the characteristics of the bond issue: in fact SPV raises capital on the market by issuing catastrophe bonds. When a risky event takes place within a specified risk period, the risk benefit to be paid to the investors, in terms of interests, capital or both, is reduced according to the losses suffered by the sponsoring firm. The resources made available on the market, the returns deriving from their investment and the premiums paid by the issuer are the incoming entries of SPV, necessary to comply with the commitments with the bondholders and the compensation to be paid to the sponsoring firms in the event of a claim. At least in part, the two output items are alternatives, given that in the absence of a catastrophic event the SPV must satisfy the investors entirely; otherwise, the investors stand reductions in proportion to the losses and the sponsoring firm is compensated.

5.5 Conclusions

A comprehensive approach to operational risk management requires also appropriate risk mitigation and/or transfer strategies. Particular consideration must be given to the extent to which risk mitigation tools truly reduce risk, transfer the risk to another business sector or area, or create a new risk (e.g. counterparty risk).

Noteworthy developments could result in product innovation that would make insurance even more effective as surrogate capital supporting operational risk. As a related matter, banks could be required to systematically track details of coverage, terms and conditions, both to improve modelling of insurance recoveries, and to facilitate that product innovation.

Risk transfer or insurance is recognized by the regulator as a mitigation method only for the advanced approach (subject to a ceiling of 20% of operational risk capital) and, to be eligible for capital at risk recognition, an insurance policy must be compliant with specific requirements. This has underlined the strategic importance of insurance portfolio management in banks. The development of the opportunities

of insurance tools within the operational risk management may in fact contribute in reducing the capital charge and the economic impact linked to the operational losses.

Nevertheless, there are several challenges with the use of insurance. Among others, there is the difficulty in measuring (modelling) the extent of insurance's mitigating effect, a pre-condition for any bank's claim against capital. Moreover, AMA models are generally constructed around the Basel event types, while insurance programmes are built around discrete coverage: unfortunately the two taxonomies are often incompatible with one another.

References

Bazzarello, D., B. Crielaard., F. Piacenza., and A. Soprano. 2006. Modeling insurance mitigation on operational risk capital. *Journal of Operational Risk*, March.

BCBS (Basel Committee on Banking and Supervision). 2009. *Results from the 2008 loss data collection exercise for operational risk*, July.

BCBS (Basel Committee on Banking and Supervision). 2010. *Recognising the risk-mitigating impact of insurance in operational risk modelling*, October.

Blacker, K. 2000. Mitigating operational risk in British retail banks. *Risk Management* 2 (3).

EBA (European Banking Authority). 2015. *Final draft regulatory technical standards on the specification of the assessment methodology under which competent authorities permit institutions to use advanced measurement approaches (AMA) for operational risk in accordance with Article 312 of Regulation (EU) No 575/2013*, June.

Franzoso, F. 2005. La copertura dei rischi operativi mediante strumenti assicurativi. Corso di aggiornamento ASSBB—Università Cattolica su Il rischio operativo nelle banche: metodologie di valutazione e strumenti di copertura assicurativa, 7–8 Giugno, Milano.

KPMG. 2008. *Basel implementation worldwide*, January.

Kuritzkes, A.P., and H.S. Scott. 2005. Sizing operational risk and the effect of insurance: Implications for the Basel II capital accord. In *Capital adequacy beyond Basel: Banking, securities, and insurance*, ed. H.S. Scott. Oxford University Press.

Lemmi Gigli, N. 2005. Trasferimento del Rischio Operativo. V Convention Aifirm, Convegno Nazionale Risk Management, 20–21 Ottobre.

Li J., S. Yi., J. Feng., and Y. Shi. 2011. Modelling the mitigation impact of insurance in Operational Risk management. *Procedia Computer Science* 4: 1668–1674.

Locatelli, R. 2001. I rischi operativi: I temi sul tappeto. In R. Locatelli, E. Magistretti, P. Scalerandi, and G. Carosio, Il rischio operativo, Giornate Romane dell'ASSBB, Roma, 9 Novembre, Quaderno n. 193.

Marzano, A. 2005. Il rischio operativo nelle banche: metodologie di valutazione e strumenti di copertura assicurativa, Corso di aggiornamento ASSBB—Università Cattolica su Il rischio operativo nelle banche: metodologie di valutazione e strumenti di copertura assicurativa, 7–8 Giugno, Milano.

Mendolia, A. 2001. Soluzioni alternative di trasferimento del rischio nel settore assicurativo. *Amministrazione & Finanza*, n. 7.

Miani, S. 2004. *La gestione dei rischi climatici e catastrofali*. Torino: Giappichelli.

Peters, G.W., A.D. Byrnes., and P.V. Shevchenko. 2011. Impact of insurance for operational risk: Is it worthwhile to insure or to be insured for severe loss? *Insurance: Mathematics and Economics* 48, 287–303.

Pisani, R. 1996. Il processo di gestione: le politiche di finanziamento del rischio. In Risk management. Strumenti e politiche per la gestione dei rischi puri d'impresa, ed. G. Forestieri. Milano: Egea.

Scott, H.S., and H. Jackson. 2002. *Operational risk insurance—Treatment under the new Basel Accord*. Aino Bunge International Finance Seminar. Springer.

Sironi, A. 2003. Il rischio operativo: una nuova sfida per le banche italiane, Economia e Management, n. 1.

Sironi, A., and A. Resti. 2008. *Rischio e valore nelle banche*. Milano: Egea.

Tagliavini, P. 1994. *La captive insurance company come strumento di risk management*. Milano: Egea.

Vellella, M. 2005. La gestione dei rischi operativi nelle banche: Alcuni spunti di riflessione sulle scelte organizzative. *Banche e Banchieri*, n. 3.

6

Operational Risk Modelling: Focus on the Loss Distribution and Scenario-Based Approaches

6.1 Introduction

The degree of flexibility that banks have had in operational risk modelling has fostered over the years the development of a variety of methods. Currently, these may be related to two categories, namely the loss distribution approach and the scenario-based approach.

This chapter aims at analysing the specific features of both the methodologies, highlighting strengths and weaknesses of each one. As it is not possible to state which approach is the best in absolute terms, according to the best practices, the combined use could be the preferable choice.

6.2 The Loss Distribution Approach

The degree of flexibility that banks have had in operational risk modelling has fostered over the years the development of a variety of methods. Initially distinguished as the Internal Measurement Approach (IMA),[1] the Scorecard Approach (SA)[2] and the Loss Distribution Approach (LDA), these methods have been recently reduced to two categories, namely the LDA and the Scenario-Based Approach (SBA). While the

G. Birindelli and P. Ferretti, *Operational Risk Management in Banks*,
Palgrave Macmillan Studies in Banking and Financial Institutions,
DOI 10.1057/978-1-137-59452-5_6

former is based on real loss, and the other on the expected loss, the use of a joint approach is not excluded as the information gathered from one method can complement the information obtained by the other, and vice versa.

In general, the models based on the LDA (see among others Dutta and Perry 2013), featuring a quantitative output, allow to estimate the expected loss directly and to increase the sensitivity of the capital requirement in relation to the intermediary's true operational risk exposure (Lemmi Gigli 2005; Savelli 2005; Guray Uner 2008). The LDA is a statistical method, widespread in the actuarial setting, that allows to calculate—starting from internal and external loss data and for each combination of BL-risk factors—both a frequency and a severity distribution. The frequency distribution is the function of discrete density that expresses the number of loss events during a specific timeframe, while the severity distribution is a function of continuous density, which provides information on the event's impact in terms of financial loss: by joining the (presumably) independent distributions, we obtain an aggregated distribution of losses. This latter is estimated for each BL, in order to obtain, through the sum of each Value at Risk (VaR), the definition of the total capital requirement. It is understood that the simple addition presupposes that the classes of events result perfectly correlated among each other, unless one turns to alternative aggregation procedures that can take correlation hypotheses into account.

Although LDA models presuppose some flexibility in their implementation, there are several common elements shared by many methods linked to this model family (Bazzarello and Piacenza 2009). Such common elements (which will be dealt with in more detail in the next Sections) can be linked to the following:

- Calculation dataset
- Classes of operational risk
- Estimate of the loss severity distribution
- Estimate of the loss frequency distribution
- Distribution of yearly aggregate losses
- Risk class aggregation
- Calculation for risk capital.

6.2.1 Calculation Dataset

The *calculation dataset* refers to the set of available data used for the OR capital requirement. Its creation relies on the fundamental activation of procedures and software applications that allow the BUs involved to insert their losses in a centralized database. This generally involves also the use of external loss data (i.e. taken from external sources) as well as of scenario analysis based on expert opinions.

The dataset of internal losses is made up by the bank's loss data and represents the main element in each LDA-like model. It generally includes information on the description of the event; the company (or other internal structure, such as sub-holding or business unit) that is hit by the loss; the overall loss caused by the event (sum of economical manifestations relevant for the loss); the date of occurrence; the date of detection; the date of accounting; the business line; the type of event; the potential crossing with other types of risk (e.g. market risk, credit risk).

Generally, each element within the internal loss dataset is composed of an operational event, such as a robbery, which is connected to a range of economical manifestations (damage caused to break in, loot, recovery) that must be aggregated within the overall loss. For the purpose of establishing the operational loss deriving from an event, the manifestations considered relevant are those which can have a negative impact such as losses and provisions. These can be subtracted from the recoveries, if they occur within a short time from the occurrence of the operational event. In such case, they are considered immediately recovered losses.

The loss events considered must fall within the observation period, i.e. the timeframe considered relevant for the calculation dataset. Legislation on the matter requires this timeframe to be at least of 5 years—or exceptionally of 3 years in the initial period the model is applied.

As for the observation period, there is still no shared rule on the relevant date but rather refer to a number of different types of dates relating to the operational risk event: occurrence date, detection date, accounting date, upload date, etc. In general, the date of occurrence can be considered reliable for the bank's risk profile, although not all events may fall

within the dataset as, for example, in the case of a lawsuit due to internal fraud where the date of occurrence of the event and the date of effective loss can be years apart. If this time lapse were longer than 5 years, this event might indeed not fall within the dataset used for the calculation. Hence, especially from the regulator's point of view the date of detection and of accounting might be preferable. Yet, while the accounting date can be confirmed more easily and recovered within the bank, the date of detection may be more difficult to confirm. In any case, the choice of the accounting date is quite conservative: theoretically, it would be possible to include in the dataset losses that have occurred many years earlier and which no longer represent the bank's risk profile. In this case it may be useful to set a period of observation for the date of occurrence as well as the one defined for the accounting date.

The relevant date for the purposes of calculating the capital requirement is not the only hurdle involved in identifying the correct database. Indeed, operational losses often show a number of economic impacts that can stretch over a number of years. Therefore it is important to understand how they can be aggregated. Among the several options, one could be articulated with the following steps:

- Consider only the economic impacts relating to the validated events (in the case of the establishment of a validation and control process for operational events)
- Take into consideration all the economic impacts recorded during the observation period
- Adjust the amounts of economic impacts for inflation
- Calculate the total operational loss of the event as the sum of losses, provisions and recoveries, considering the losses and provisions as a positive and recoveries negative. In this step it is also possible that the bank deduct the losses promptly retrieved. If the same operational event impacts on different companies, each of them should report the event and the economic impacts falling under its competence. These events must then be aggregated into a single multiple event having as total loss the sum of the losses of the single events by which it is composed. In general, even different operational events that are apparently interdependent should be aggregated into a single

loss. On the other hand, operational events from different risk classes should not be aggregated, unless the bank decides to assign the entire multiple event to the risk class in which it has the greatest impact
- Once the aggregation process ends, select operational events having total losses higher or equal to the minimum threshold considered
- Exclude cross-operational events with credit risk.

For what concerns the dataset of external losses, we must emphasize that the purpose of the use of external data is to complement data on events with low frequency and high severity which internal data alone could not provide. External data can be retrieved either from consortium databases (such as the DIPO, the Italian database of operating losses at national level and the ORX Operational Risk eXchange at international level) or from public databases such as the Algo OpData (Bazzarello and Piacenza 2009).

The external data used, however, must be consistent with internal data in order to be suitable for inclusion into the calculation dataset. This requires establishing internal processes that focus on and verify the consistency of classifications of external and internal data. Accordingly, cross-operational events with credit risk and events having a date outside of the observation period, for example, would be excluded from the dataset.

One of the major problems in the treatment of the external data is to determine whether and how they should be subject to scaling (on the topic consult, among others, Torresetti and Nordio 2014; Abdymomunov and Curti 2016). In fact, external data must be treated appropriately, in order to increase the accuracy and robustness of the estimates without undermining the model's results due to inconsistencies with internal data. The main approaches employ as scaling factors some dimensional indicators, such as intermediation margin, number of employees and number of branches. In particular, there has been the proposal of a scaling rule based on the linear correlation between the logarithm of the losses and the logarithm of the dimensional indicator (Shih et al. 2000). However, the correlation estimates obtained are generally very low, for which the external data scaled in fact remain unchanged compared to the original values.

These results show that the dimensional indicators may be not entirely suitable for the scaling of the external data. An alternative would be to use indicators related to the statistical properties of the data, such as the mean or median. On the other hand, any scaling methodology can be viewed as manipulation of data, aimed to influence the results as wanted. It is also noteworthy to mention that even the internal data of a bank come from subsidiaries differ in both size and activity; hence, on the basis of the logic of the external data scaling, so should internal data be scaled as well. In light of these considerations, it might be preferable not to scale external data, in favour of the construction of a computational model that can treat them appropriately using their original amounts.

6.2.2 Classes of Operational Risk

Besides the definition of the calculation database, another central element of LDA type models is the determination of the model's granularity. This essentially means determining what granularity to use for modelling data and thus establish the procedures for identifying the risk classes. The loss data should in fact be divided into homogeneous categories that internally satisfy the i.i.d. hypothesis. Such classes are known as OR classes and their number determines the greater or lesser granularity of the model.

In particular the OR class is defined as a homogeneous category in terms of risks included and data available for the analysis. Some examples of classes of risk are event type, business line, combination event type/business line, society and cause.

When an LDA model is applied, it is assumed that the data belonging to the same class of risk are independent and identically distributed. The legislation requires testing these hypotheses for the data belonging to the same class of OR as a prerequisite for robust modelling. Below, we describe some useful techniques for these purposes and for the purposes of homogeneity and independence, as well as any seasonal and stationary trends (Bazzarello and Piacenza 2009).

For the purposes of the identical distribution of risk classes, it is necessary to emphasize that an OR class is a risk category composed

of homogeneous data. The identification of classes must consider the trade-off between homogeneity and availability of data. In fact, increasing the number of classes (i.e. the granularity of the model) increases homogeneity, but lowers the amount of data available for the estimates in each class; by contrast, decreasing the number of classes increases the data available, but the data in each class are less homogeneous.

As it is well known, one of the requirements of the AMA models is to classify the data on losses gathered by type of event and BL, the combination of which may be regarded as minimal risk class, thus ensuring a high degree of homogeneity. This classification is, however, difficult to apply in the calculation model, due to insufficient data available for some classes. One possible solution could be classifying the data either by type of event or by business line alone. In this case, the availability of the data would no longer be critical but would still require homogeneity be verified by means of grouping analysis (cluster analysis). Starting from n elements, performing $n-1$ consecutive aggregations leads to a single group. In order to do this, a measure of dissimilarity between the elements must be defined (Bazzarello and Piacenza 2009). In this case the n elements are the minimal risk classes BLxET, while the measure of dissimilarity between elements i and j can be defined as

$$d(i,j) = 1 - pv(i,j)$$

where *pv(i,j)* represents the *p*-value of the Kolmogorov–Smirnov test applied to samples i and j. This test, in the two-sample version, assesses whether these have the same probability distribution. Accordingly, this tests the hypothesis:

$$H0 : F1(x) = F2(x) \forall x$$
$$H1 : F1(x) \neq F2(x) \text{ for at least one value of } x$$

This uses the statistics $T = \sup x\_ F1\ (x) - F2\ (x)\_$, the greatest vertical distance between two functions of empirical probability. Applying this algorithm to each of the $n-1$ iterations, the distances between all residual groups are calculated and the groups having the minimum distance are aggregated into a single group. The distances between the groups can be calculated with the method of the means: the distance

between two groups is defined as the mean of the dissimilarity between the elements of a group and the elements of the other group.

In order to choose between classification by event type or BL, the level of aggregation of the minimal classes BLxET can be tested in two ways:

- business lines are considered as risk classes. The purpose is to determine the level of dissimilarity at which the aggregation is affected between the BLxET cells that form each individual business line: $\left(d_1^{\mathrm{BL}}, \ldots, d_8^{\mathrm{BL}}\right)$
- event types are considered as risk classes. The purpose is to determine the level of dissimilarity at which the aggregation is affected between the BLxET cells that form each event type $\left(d_1^{\mathrm{ET}}, \ldots, d_7^{\mathrm{ET}}\right)$.

One criterion for selecting one of the two classifications might be comparing the highest among the aggregate distances obtained for the type of event and the highest among the aggregate distances obtained for the business lines. Therefore, the classification by type of event is preferred if: $\max\left(d_1^{\mathrm{ET}}, \ldots, d_7^{\mathrm{ET}}\right) < \max\left(d_1^{\mathrm{BL}}, \ldots, d_8^{\mathrm{BL}}\right)$.

Conversely, the classification for business line will be used. The results of each cluster analysis can be represented by graphs known as dendrograms.

To increase the homogeneity of the data from a temporal point of view, it is useful to consider the effect of inflation (Bazzarello and Piacenza 2009). To this end, each loss included in the calculation dataset can be scaled, for example, from the CPI (Consumer Price Index) on a monthly basis. It may be worth considering as a reference date the date of accounting of the event, although other dates could be used in case of unavailability (e.g. occurrence, detection). The loss adjusted for inflation can be calculated as follows:

$$A' = A \times \frac{\mathrm{CPI}(M_{\mathrm{RD}})}{\mathrm{CPI}(M_{\mathrm{AD}})}$$

where,

A is the original loss amount

A' is the loss adjusted for inflation

M_{RD} is the month to which the calculation refers to (generally the end of the observation period)
M_{AD} is the month to which the loss refers to
$\text{CPI}(M_{RD})$ is the CPI value for the M_{RD}
$\text{CPI}(M_{AD})$ is the CPI value for the M_{AD}

For the consistency of the model it is important that the adjustment for inflation be applied also to the minimum loss detection threshold, so that events relating to past years, and that had not been considered before because of the lowest amount, do not exceed the threshold only for the effect of inflation.

Once homogeneity has been considered, it is necessary to test the hypothesis of independence of loss data within a same risk class. When referring to the dependence of the data in a same class we speak of implicit correlation in order to distinguish with respect to the correlation between different classes (explicit correlation). Intuitively, the dependence in the same class of risk should be greater than the dependence between different classes, since data belonging to a same category are more similar by definition. Nevertheless, academia and regulators have devoted more attention to the explicit correlation.

The independence of the data in the same risk class can be analysed using autocorrelation graphs applied to loss data sorted by date. If the data were to show a significant level of autocorrelation for some time delay, it would be necessary to aggregate the dependent events in a single total loss. Since the uniformity in the definition of risk classes had previously been addressed, the requirement of identical distribution of risk class would have to be reasonably verified (Bazzarello and Piacenza 2009).

Finally, in applying the classical LDA models, it is assumed that the data analysed are stationary: that is, it is given that the estimated parameters are independent of the time (data do not feature temporal trends). The non-stationarity of data can be detected applying the smoothing functions to the time series of annual losses aggregated both in terms of severity and frequency, in order to facilitate the detection of trends. In the event non-stationarity is detected, the model needs to be modified to yield the correct estimate of risk capital, increasing for example the weight of the latest data in parameter estimates. On the other hand, the

scarce profoundness of the time series available does not allow detecting these behaviours with a high degree of confidence.

As to the season trends—that is the cyclical behaviour of data—this can be detected by using autocorrelation graphs applied to aggregated losses over different periods (week, month, trimester, year, and so on). Considering that the operational risk capital is measured on a yearly basis, the seasonal trend on shorter periods is non-relevant. On the other hand, the seasonal trend at annual level can be barely appreciated because of the shallow deepness of the time series.

6.2.3 Estimate of the Loss Severity Distribution

The probability distribution of the individual loss is estimated for each class of risk. Typically, this is performed through the application of parametric models, i.e. probability function having a number of parameters (usually 2–4) that identify the type. The parameters are estimated on loss data belonging to the class analysed employing one of the methods available (for example, maximum likelihood). The choice of both the parametric model and the method for estimation of parameters must be made in a way that will yield the best possible fit to the data loss. This point is crucial in the implementation of an LDA model, since an incorrect determination of the severity distribution, especially in the tail area, can lead to a non-reasonable estimate of risk capital.

One of the main issues with LDA models is therefore the correct identification of the severity distribution, herein defined as a continuous random variable X and described with the function $f_X(x, \theta)$, where θ is the parameter or the vector of the parameters (Bazzarello and Piacenza 2009).

To select the distribution that best fits the data loss, both analytical and graphical methods are available. Among the graphical methods, the most widely used is the quantile–quantile plots (q q-plot), which allows assessing the goodness-of-fit of data in the distribution tail, the part that most influences the estimation of risk capital. The method consists in comparing graphically the empirical and the estimated quintiles.

Given the orderly samples of losses $x_{(1)} \leq x_{(2)} \leq \cdots \leq x_{(n)}$, the graph is built representing the following points:

$$\left\{ \left(x_{(i)}, F^{-1}\left(\frac{i}{n+1} \right) \right) : i = 1, \ldots, n \right\}$$

If the points represented fall around the bisector, that means there is a good fit to data.

If the loss data are collected only above the threshold H, the points to represent are the following:

$$\left\{ \left(x_{(i)}, F^{*-1}\left(\frac{i}{n+1} \right) \right) : i = 1, \ldots, n \right\}$$

where:

$F^*(x) = \begin{cases} \frac{F(x)-F(H)}{1-F(H)} & x \geq H \\ 0 & x < H \end{cases}$ is the function of conditional probability for the left-truncation;

$F^{*-1}(p) = F^{-1}(p(1 - F(H)) + F(H)) \;\; 0 \leq p \leq 1$ is the conditioned quantile function for the left-truncation.

Among the analytical models, we shall remember the goodness-of-fit tests of Kolmogorov–Smirnov and of Anderson–Darling. Supposing that the sample $x_1, \ldots, x_n$ is the creation of random variables having identical distribution of risk classes with a cumulative probability function $F(x)$, we test the following hypotheses:

H_0 (main hypothesis): the sample shows a cumulative probability function $F(x)$

H_1 (alternative hypothesis): the sample's distribution is not function of cumulative probability $F(x)$

The statistics of the goodness-of-fit test is a measure of the distance between the empirical probability function and the estimated probability function.

The Anderson–Darling is more useful for measuring OR, since it gives a greater weight to the distribution tail. If the data are truncated to

the left with an H threshold, the probability function $F(x)$ needs to be replaced with the conditioned function for left-truncation $F^*(x)$.

To evaluate the test result, we may calculate the *P-value*, that is the value by which 1−(*P-value*) is the maximum confidence level by which the main hypothesis can be rejected. Hence, the greater the *P-value*, the better the data fit to the distribution. Accordingly, the best distribution among those tested will be the one presenting the greatest *P-value*. The computation of the *P-value* can be achieved by the Monte Carlo simulation (Chernobai et al. 2005) or the use of pre-computed tables, and in any case, using the most common statistics programs.

The selection of the best distribution should be done with the joint use of graphical and analytical methods, while avoiding automatic methods since, for example, the change of distribution between two consecutive analyses could compromise the stability of the results.

In estimating the severity of the operational losses, determining a distribution that will fit well data in both "body" and tail can be complex. Therefore, it might be useful using two different distributions for estimating the severity: one representing the low-impact high-frequency losses, i.e. the "body"—and another the high-impact low-frequency losses, i.e. the tail. The tail can be estimated by considering the Extreme Value Theory (EVT).

Let X be a random variable having cumulative probability function *F*. Given the threshold *u*, the excess distribution function over *u* is

$$F_u(y) = \Pr(X - u \leq y | X > u).$$

For a broad class of functions *F*, the limit distribution for $u \to \infty$ of the excesses is called the Generalized Pareto distribution (GPD), and is as follows:

$$G(x;\xi,\mu,\beta) = \begin{cases} 1 - \left(1 + \xi \frac{x-\mu}{\beta}\right)^{-1/\xi} & \text{if } \xi \neq 0 \\ 1 - e^{-(x-\mu)/\beta} & \text{if } \xi = 0 \end{cases} \quad \text{where :} \quad \begin{array}{ll} x \geq 0 & \text{if } \xi \geq 0 \\ 0 \leq x \leq \mu - \frac{\beta}{\xi} & \text{if } \xi < 0 \end{array}$$

The function of probability is

$$g(x;\xi,\mu,\beta) = \begin{cases} \frac{1}{\beta}\left(1 + \xi \frac{x-\mu}{\beta}\right)^{-\frac{1}{\xi}-1} & \text{if } \xi \neq 0 \\ \frac{1}{\beta} e^{-(x-\mu)/\beta} & \text{if } \xi = 0 \end{cases} \quad \text{where :} \quad \begin{array}{ll} x \geq 0 & \text{if } \xi \geq 0 \\ 0 \leq x \leq \mu - \frac{\beta}{\xi} & \text{if } \xi < 0 \end{array}$$

where $\xi \in R$ and $\beta > 0$ are the parameters shape and scale, respectively. μ is the location parameter set equal to the threshold u ($\hat{\mu} = u$). If $\xi > 0$ then distribution is said to be thick tailed, as in most cases of operational risks (Embrechts 2000).

The EVT approach requires the definition of a threshold u, beyond which observations are considered as extreme. Such choice is pivotal since it determines the number of observations useful for the estimation and the quality of the observations exceeding the threshold.

In fact, too low a threshold implies the use of a high number of observations, but at the same time does not guarantee that such observations are extreme data, increasing the distortion; too high a threshold should ensure that the exceeding observations are extreme values, yet their limited number reduces the quality of the estimates, increasing the variance.

An appropriate threshold value can be determined using the graph of the empirical function of the mean of the excesses, which, in addition to a high enough threshold value, should follow a linear behaviour:

$$e(u) = E(X - u|X > u) = \frac{\beta + \xi u}{1 - \xi}$$

Once the threshold is identified, the GPD parameters can be determined using the method of maximum likelihood or, in the case in which very limited data is available (frequent for operational risks) using the Probability Weighted Moments (PWM) method instead. This method (PWM) ensures a better robustness of the estimates and a greater stability compared to variation of the threshold (Hosking and Wallis 1987).

In literature there are many examples which suggest applying EVT for OR measurement (Aue and Kalkbrener 2007; Chapelle et al. 2004; Moscadelli 2004; Romano and Di Clemente 2003). Conversely, other authors (Dutta and Perry 2013; Mignola and Uguccioni 2005) highlight the issues that may be encountered using this method, such as the lack of fit to data, the instability in relation to the variation of the threshold, the calculation of results which are too conservative.

6.2.4 Estimate of Loss Frequency Distributions

For each risk class, the probability distribution of the numerosity of annual losses is determined. Usually the simpler models such as the Poisson distribution are used (Bazzarello and Piacenza 2009).

6.2.5 Distribution of Yearly Aggregate Losses

For each risk class, the probability distribution of annual losses is determined starting from the severity and frequency distributions. Because it is not possible to represent this distribution by means of a closed shape, numerical techniques such as the Monte Carlo simulation, are used instead (Bazzarello and Piacenza 2009).

6.2.6 Risk Class Aggregation

The total risk capital can be calculated simply as the sum of the various risk capitals for all classes.

Defining $VaR(h)$, $h = 1, 2, \ldots, H$ as the Value at Risk (VaR) calculated on the distribution of losses relating to class h, then

$$VaR(total) = \sum_{h=1}^{H} VaR(h)$$

Using this method is equivalent to assuming that the various classes of risk are perfectly dependent. It is reasonable to think that this assumption is too conservative and that there is diversification across risk classes. One method for incorporating the diversification effect is based on the use of the copula function (e.g. Gaussian, Student's or Archimedean).

Let $X = (X_1, \ldots, X_n)$ be the vector of the n random variables, with marginal probability function $F_1, \ldots, F_n$. The multivariate probability function:

$$F(x_1, \ldots, x_n) = P[X_1 \leq x_1, \ldots, X_n \leq x_n]$$

determines full the dependence structure of the variables $X_1, \ldots, X_n$.

However, because its analytical representation is often too complex, it is practically impossible to estimate and to use it in the models.

The use of the copula function allows overcoming the issue of estimating the multivariate probability function in the following way: first we determine the marginal probability functions $F_1, \ldots, F_n$ representing the distributions of each random variable; then we determine the dependency structure of the variables $X_1, \ldots, X_n$ by specifying an appropriate copula function (Bazzarello and Piacenza 2009).

An n-dimensional copula is a multivariate probability function C with marginal functions distributed evenly [0,1] ($U(0, 1)$), so that

1. $C : [0, 1]^n \rightarrow [0, 1]$;
2. C has marginal functions C_i so that $C_i(u) = C(1, \ldots, 1, u, 1, \ldots, 1) = u \, \forall u \in [0, 1]$.

Therefore, if $F_1, \ldots, F_n$ are univariate distribution functions, $C(F_1(x_1), \ldots, F_n(x_n))$ is a function of multivariate distribution with marginal functions $F_1, \ldots, F_n$, since $u_i = F_i(x_i)$, $i = 1, \ldots n$ is a uniform random variable. Accordingly, the copula functions can be used to build and simulate multivariate distributions.

The following theorem is crucial to the practical application of copula functions (Sklar 1959). If F is a function of n-dimension probability marginal functions $F_1, \ldots, F_n$, then it has a single representation through the copula function:

$$F(x_1, \ldots, x_n) = C(F_1(x_1), \ldots, F_n(x_n))$$

From this theorem we see that for continuous multivariate probability functions:

- univariate marginal functions and multivariate dependence structure can be separated;
- the dependence structure can be represented through an appropriate copula.

From Sklar's theorem we derive the following corollary. Let F be a distribution function with n-dimensional continuous marginal functions $F_1, \ldots, F_n$ and copula C (which satisfied the theorem). Then

$$C(u_1, \ldots, u_n) = F(F_1^{-1}(u_1), \ldots, F_n^{-1}(u_n)) \qquad \forall \mu = (u_1, \ldots, u_n) \in [0,1]^n,$$

where F_i^{-1} is the inverse of F_i.

The following sections describe some of the main copula functions used to measure operational risks.

The Gaussian copula (or normal) is the copula of the multivariate normal distribution. In fact, if the random vector $X = (X_1, \ldots, X_n)$ is composed of independent and normally distributed variables:

- the univariate marginal functions $F_1, \ldots, F_n$ are Gaussian;
- the dependence structure between the marginal distributions can be described by a single copula C_R^{Ga} (The Gaussian copula), so that

$$C_R^{\mathrm{Ga}}(u_1, \ldots, u_n) = \Phi_R(\phi^{-1}(u_1), \ldots, \phi^{-1}(u_n)),$$

where Φ_R is the function of the multivariate standard normal probability function with correlation matrix $R = \{\rho_{ij}\}$ and ϕ^{-1} is the inverse of the standard univariate Gaussian probability function.

The Gaussian copula parameter can be estimated deriving it from Kendall's correlation coefficients, applying the following transformation:

$$\rho = \sin\left(\frac{\pi}{2}\rho_\tau\right),$$

where ρ_τ is Kendall's coefficient and ρ is the correlation coefficient used as the Gaussian copula parameter. The matrix obtained could be non-semidefinite positive. In such case we shall apply a transformation based on the eigenvalues method (McNeil et al. 2005).

In order to simulate random variables of the Gaussian copula, the following procedure is followed.

If the matrix R is positive-definite, there is a matrix A sized $n \times n$ so that $R = AA^T$. Moreover, we suppose that the random variables $Z_1, \ldots, Z_n$ are normal independent standards. Then, given the vector $\mu \in R^n$, the random vector $\mu + AZ$ (where $Z = (Z_1, \ldots, Z_n)^T$) is multinormal, with mean vector μ and covariance matrix R. The

matrix A can be established easily applying the Cholesky factorization to the matrix R. This yields an individual lower triangular matrix L so that $LL^T = R$. Therefore, random variables can be generated by the n-dimensional Gaussian copula using the following algorithm:

- apply the Cholesky factorization A to the matrix R;
- simulate the determinations of n independent standard normal random variables $z_1, \ldots, z_n$;
- pose $x = Az$;
- determine the components $u_i = \phi(x_i), i = 1, \ldots, n$;
- the resulting vector, $(u_1, \ldots, u_n)^T$ is the creation of a n-dimensional Gaussian copula, C_R^{Ga}.

Likewise, the t is the copula function of the multivariate Student distribution.

Let $X = (X_1, \ldots, X_n)$ be a random vector with multivariate t distribution with ν degrees of freedom. The copula of the vector X can be represented as follows:

$$C_{\nu,R}^t(u_1, \ldots, u_n) = t_{\nu,R}(t_\nu^{-1}(u_1), \ldots, t_\nu^{-1}(u_n))$$

where R is the correlation matrix.

$t_{\nu,R}^n$ denotes the multivariate probability function of the random variable $\sqrt{\nu}Y \Big/ \sqrt{S}$. The random variable $S \sim \chi_\nu^2$ and the vector Y are independent.

t_ν denotes the margins of $t_{\nu,R}^n$.

The R correlation matrix for the Student's t copula can be estimated in the same way as the Gaussian copula, while the number of degrees of freedom ν can be determined using the maximum likelihood method.

To carry out random sampling by Student's t copula we can use the following algorithm:

- perform a Cholesky factorization A of R;
- simulate n random independent variables $z_1, \ldots, z_n$ from the standard normal distribution;
- simulate a random variable, s, from the distribution χ_υ^2, independent from z;

- determine the vector $y = Az$;
- calculate $x = \frac{\sqrt{\upsilon}}{\sqrt{s}} y$;
- determine the components $u_i = t_\upsilon(x_i)$, $i = 1, \ldots, n$;
- the resulting vector, $(u_1, \ldots, u_n)^T$, represents a random simulation from a n-dimensional copula ${}_t C^t_{\upsilon,R}$

It is generally believed that the fit of data to Student's t copula is better than the fit to the Gaussian copula. This is due to the capability of copula t to capture the dependency between extreme events. Such property is called tail dependence. Moreover, the copula t represents a generalization of the Gaussian copula, as it can be linked to it in the events the number of degrees of freedom ν tend to $+\infty$ (Aas 2004; Demarta and McNeil 2005; Romano 2002; Romano and Di Clemente 2003).

The copula's dependency parameter can be estimated with a rank correlation (e.g. Kendall, Spearman), since the more traditional linear correlation (Pearson) sets the hypothesis of normality of the random variables, which is not realistic in the case of operational risk. Alternatively, it is possible to estimate parameters using the maximum likelihood method. As the requirement needs to be determined on a one year time horizon, accordingly the dependency structure shall be identified on a yearly level. However, the scarce deepness of the time series available for OR would not allow an accurate and robust estimate. Another alternative would be to estimate the correlation by month. In fact, if there is not a dependency between the monthly aggregate losses in each category of risk, the same dependence structure can be transposed at annual level (Chapelle et al. 2004). To verify that the transposition can be truly made for a certain class of risk, an analysis of autocorrelation between the monthly losses can be performed. If there are no significant autocorrelations when repeating the analysis for each class, the estimated correlation at monthly level can be used without distorting the final results.

To determine the distribution of the total annual losses, considering the exact structure of dependence between the risk classes through a copula function, the Monte Carlo simulation can be used. It is given that the yearly cumulative probability distributions $F_{S(h)}$, $h = 1, \ldots, H$ have already been obtained for each risk class.

The distribution function of the total annual losses is obtained by the following steps, that shall be repeated a high number of J times (for example $J = 1.000.000$):

- generate a representation of the random multivariate vector $\bar{u} = (u_1, \ldots, u_H)$ with uniformly distributed marginals on [0,1] by a determined copula C;
- this yields a loss scenario for each type of risk $s_j(h),\ h = 1, \ldots H$ by applying to the representation above the inverse cumulative probability distribution $F_{S(h)}\left(s_j(h) = F^{-1}_{S(h)}(u_h)\right)$;
- this yields a scenario for the total annual loss, $s_j(\text{total})$, summing the losses $s_j(h)$ for each $h = 1, \ldots H$, that is: $s_j(\text{total}) = \sum_{h=1}^{H} s_j(h)$.

This results in a simulated empirical distribution of the total losses, from which the total VaR can be calculated as 99.9% quantile (see below).

6.2.7 Calculation for Risk Capital

Once the total annual loss distribution has been calculated, the risk capital can be calculated using a measure of risk. The most used measure in the finance field is the VaR. The VaR with confidence level α is defined as quantile of level α $(0 < \alpha < 1)$. In the case of ORs, capital charges must be calculated considering a one year time horizon and a confidence interval of 99.9%. Accordingly, the risk capital can be determined as VaR with a 99.9% confidence level calculated on the distribution of the total annual losses (Bazzarello and Piacenza 2009).

6.3 The Scenario-Based Approach

In the scenario-based models the capital estimate for operational risk is achieved by means of subjective assessment, rather than by means of loss data.

The scenario-based approach (SBA) literature documents widespread convergence for the meaning of the term "scenario" as the description of a possible sequence of events that includes an assessment of the likelihood of the event occurring and an estimate of the severity of the expected adverse consequences (Laycock 2014). Therefore, each risk scenario should describe a risk event, the likelihood of its occurrence, and its financial impact on the company. Other definitions describe scenarios as plausible alternatives about the future environment or, as "purposeful stories about how the contextual environment could unfold in time" (Burt et al. 2006); moreover, Lubbe and Snyman (2010) define risk scenario as a prospective risk exposure estimate. The scenario-based AMA Working Group (sbAMA Working Group 2003) distinguishes scenarios into two types (a generic scenario and a stress scenario), defined as something tangible that could happen in the future (i.e. a potential event). In particular, a generic scenario is a scenario that is derived from a generic class of scenarios (such as break-down of critical IT) by applying it to a defined area, while a stress scenario is a scenario of potentially high severity that is taken from a class of very rarely occurring potential events. Actually, the SBA can be classified as a stress testing, which is a method of exploring the effect of low probability events that lie outside the predictive capacity of any statistical model on Value at Risk (Chernobai et al. 2007). Similarly, the BIS Committee on the Global Financial System (2005) defines stress testing as "a generic term describing various techniques used by financial firms to gauge their potential vulnerability to exceptional, extreme or simply unexpected but plausible events".

Scenarios foresee assessments be made by one or more experts. The use of multiple expert assessment presents the advantage of mitigating some biases that may arise (see below), such as anchoring bias, which might occur when an individual responds alone. Yet, multiple expert assessment may present some issues, as for example the bank's burden of having to identify the method of combining these multiple assessments. In this respect, the most common methods in use are basically two (Jenkinson 2005):

- The mathematical approach, in which the assessments are first elicited individually and then aggregated using a weighting approach. The weights can depend on the level of expertise of each expert.
- The behavioural approach, which invites a group of experts to share information among themselves, and then establish a consensus assessment.

The second method is generally preferred, as it promotes discussion of operational risk between the experts and increases awareness of risk exposures for management purposes (Oakley and O'Hagan 2004).

The individuals chosen as subject matter experts should have extensive personal experience and significant knowledge and understanding of their business and the environment in which they operate. According to Segal (2011), when risk assessment is conducted by means of a survey, the participants should include the chief executive, risk, technology, financial and investment officers, heads of major business segments, heads of compliance and strategic planning as well as experienced personnel in the industry and in the company.

In the scenario-based approach, a critical feature is the involvement of a facilitator, especially for its role in providing experts a clear description of the risk's boundaries (in which risk falls within the scope of the discussion and which does not) and a definition of the process and expected outputs. Just as important is also the facilitator's ability in providing participants an effective presentation of the relevant internal and external loss data and Business Environment and Internal Control Factors (BEICFs) data, which represent an important source of information to stimulate discussion and an objective context within which the panel of experts can assess the realism of their ideas and of the estimates being generated (AG-Advanced Measurement Approaches Group 2012).

In generating relevant scenarios, a first issue is the selection of types of event to consider. One first group could be, for instance, historical events (such as unauthorized trading occurred in many banking scandals; see Chap. 2). Historical events that have taken place at other

institutions represent external data. However, generating scenario data by mainly using external data, and without considering many other hypothetical situations, may defeat the purpose of the scenario (Babbel and Dutta 2012). Therefore, the best and most widely used diffuse way is to consider a second group of scenarios: the hypothetical scenarios, which are based on some plausible risk events that have not yet occurred but which still have a non-zero probability of occurring. A scenario might also be based on the analysis of a new product that a bank will soon be offering to its clients (Rippel and Teplý 2008).

A typical problem in the assessment process performed by the participants is the existence of factors that can affect their ability to provide unbiased estimates, especially with regard to rare and large events. Namely, biases are defined as discrepancies between participants' responses and an accurate description of their underlying knowledge (Spetzler and Von Holstein 1975)[3] and are distinguished according to the following classification:

- Subconscious, or judgemental biases, if deriving from limitations in one's memory or information processing capacity.
- Conscious, or motivational biases, if arising when the participant has an interest in influencing the results of the analysis.

More specifically, biases can be distinguished as (Watchorn 2007; BCBS 2009; Gregoriou 2009):

- Availability: bias arising from the overestimation of events with which respondents had closer or more recent contact, which could thus bias the process of identifying the relevant scenarios to be assessed. Availability bias can also affect assessments on frequency of an event, which may be overstated if a relevant event is in close proximity (i.e. if the event has occurred recently in the market in which the participants operate, or if they have personally experienced one).
- Anchoring: bias arising in quantitative estimates by experts; experts start from an initial value (anchor) and then adjust it to yield their final answer. The subsequent adjustment from the anchor is typically

insufficient and leads experts to overestimate success probabilities and to underestimate failure probabilities.
- Overconfidence: bias arising from the underestimation of risk due to the small number of observed events.
- Motivational: bias arising from the misrepresentation of information due to respondents' interests in conflict with the goals and consequences of the assessment. Respondents often take on a defensive attitude when asked to estimate extreme losses for their business unit. Therefore, motivational biases can lead to the understatement of frequency and impact assessments, overstatement of the effectiveness of controls, and understatement of the uncertainty surrounding the assessments made.
- Partition dependence: bias ensuing when the respondents' knowledge is distorted by discrete choices or buckets within which their responses had to be represented; this may lead to underestimation of low-frequency events and overestimation of high-frequency events, depending on the experts' experiences.
- Framing: bias arising when outcomes from questionnaires (i.e. probability estimates) are sensitive to the phrasing and the order of questions used.
- Representativeness: bias arising when experts link the event under assessment to another similar event and hence derive their estimates from the probability of that similar event.

Scenario assessments should also be validated. A rigorous validation foresees the involvement of an independent party, who shall first confirm that the process has been carried out in all its parts and then validate the quantification results. Validation can identify and correct assessments that are illogical, inconsistent or incoherent (Clemen and Fox 2005; Oakely and O'Hagan 2004). The validator can be a person at any level of the organization: at higher level such as a Director or an Executive General Manager, lower levels (topic experts, for example from IT or HR), or transversal to the organization (such as the group operational risk function). Otherwise, the validator may be external; in either case, because the person conducting the validation may bring its own biases into the process, suitable mitigation techniques must be

enforced in order to overcome such biases. Validation can be performed relying on external loss data which can be used by the validator provided in support of validating the quantification results. As identified by the scenario-based AMA Working Group (sbAMA Working Group 2003), five techniques can be used in the validation of scenario assessments:

- the "two pairs of eyes principle";
- internal audit of the risk assessment process;
- comparison of actual losses against experts' expectations;
- comparison of the outcome of scenario assessments against internal audit findings;
- challenge by group functions such as risk.

Having a normative expert in the validation process can be crucial in identifying any biases affecting the assessments. Normative experts can look for and challenge inconsistencies, and can reveal which information is most readily available, any anchors that are being used, and whether any implicit assumptions are being made (Watchorn 2007).

In addition to validation, a reviewing process is also fundamental. In the case of regularly used scenarios the review process must pursue two objectives: determine the ongoing relevance of the scenarios and the validity of the quantification results. In the former case, it is necessary to determine whether a past scenario (created for example in the previous year) is still relevant in the current environment (as for example in the case an institution decides to revise an existing scenario which would be cheaper than creating a new one ex-novo), and whether there is a likelihood that events might still occur. In the second case, the current validity of the existing quantification results can be determined by performing comparisons with statistical distributions of losses. However, because they are by definition "backward-looking", they are unable to anticipate the current or future environment accurately. This may be partially overcome by using risk drivers: an approach often suggested is to analyse the factors that influence or drive the frequency of operational risk events and their severity (Laycock 2014).

Scenario analysis also requires expert forward-looking estimates of frequency and severity of plausible operational risk events. To this end, widely used is the quantile approach which allows estimates for specific percentiles of the frequency and severity distributions. The quantile approach typically implies experts be elicited to provide mean frequency (MF), most likely severity (MS) and worst-case severity (WS) estimates. The worst-case severity estimate is set at the 99th percentile (or higher) of the severity distribution obtained from internal or external data: the worst case is statistically defined as one of the extreme percentiles. The most likely severity estimate is set at the 50th percentile of the severity distribution (Babbel and Dutta 2012).

Questions that might be addressed to the experts are for example (Chaudhary 2014):

- What is the expected average number of loss events in a year (MF)?
- What is the most likely impact of this scenario (MS)?
- What would you judge to be the impact of the single largest event over the next 't' years (WS)?
- What would you judge to be the impact of the single largest loss out of 'x' such loss events (WS)?

The former way of eliciting WS is called "time-based elicitation", the latter "count-based elicitation". The time-based elicitation of tail quantile interlinks severity and frequency distributions, while the count-based method allows elicitation of a predetermined quantile of the individual loss severity distribution (Chaudhary 2014).

For assessing severity banks can ask the experts either to select values that correspond to specified percentiles of the underlying probability distribution, or to assess the probabilities that the true value will exceed some specified values (Kahnemann and Tversky 1974). In fact banks can use one method as main method and the other as check.

Besides, banks can ask participants to make their assessment as a point estimate or to select a quantity within the ranges where they believe the severity is likely to belong. Point estimates can generate counterfeit accuracy and the expert may become uncomfortable in trying to assess a highly uncertain value with great accuracy. The assessment in buckets

or ranges can be easier and more useful, as long as attention is drawn in constructing the ranges. Actually, if the ranges are too small, the expert may be convinced that his/her estimate falls within adjacent ranges. Conversely, if the ranges are too wide, the expert may not believe that the quantity would ever span the entire range selected (Watchorn 2007).

OeNB and FMA (2006) speak about a "scenario funnel" to indicate the spread of scenarios and the spectrum of conceivable future situations widening under the influence of incidents and interventions over time (see Fig. 6.1).

The main steps of the scenario-based approach

The scenario-based AMA Working Group (sbAMA Working Group 2003) has identified six main steps of the scenario-based approach:

1. Scenario Generation
2. Scenario Assessment
3. Data Quality
4. Determination of Parameter Values
5. Model and Parameters
6. Model Output

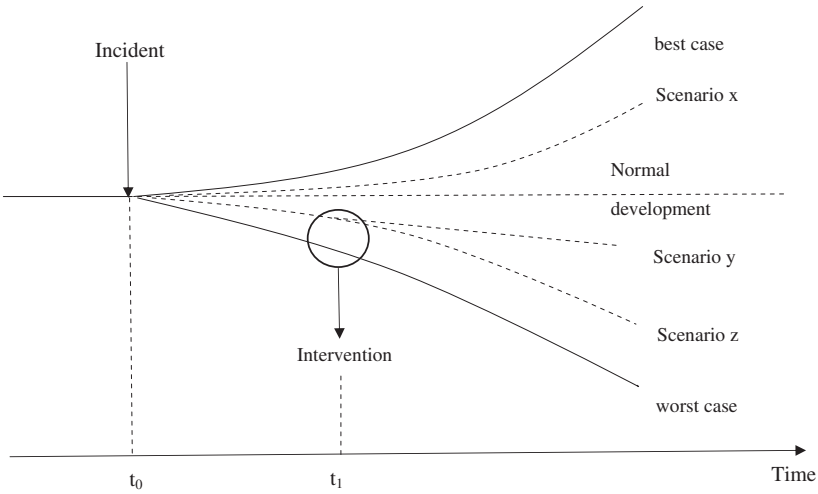


Fig. 6.1 The scenario funnel (OeNB and FMA 2006)

The first step is the scenario generation. The aim is to determine appropriate scenarios for OR and to ensure that they are consistent, relevant and capture all material ORs. During this step it is first necessary for the experts to identify all risk factors reflecting the OR profile. These risk factors can be categorized into scenario classes, which are then applied to different organizational parts, ensuring consistency across the whole organization. Finally, the scenario classes are the basis to identify the single scenarios that are relevant for the organizational part that is assessing its OR. In particular, to ensure that scenarios are consistent, relevant and fully capture all material operational risks, they must fulfil the following requirements:

- Consistent
  - Every organizational part considers as a minimum each of the common set of scenario classes, thereby achieving consistency of the overall framework
  - Techniques, such as workshops and questionnaires, allow achieving consistency of scenarios across organizational parts
  - Review by Internal Audit and Risk Function recognizes further consistency between the organizational parts
- Relevance:
  - Each organizational part assesses the relevance of all scenarios to its business and confirms its relevance (for example, if an organizational unit is not subject to IT failure, there is no need to evaluate a risk due to IT break-down).
- Full capture of all material ORs:
  - The techniques to determine the scenario classes maximize coverage of both known and expected risks.
  - Coverage is further strengthened when applied to the organizational parts and discussed with them in order to confirm that their specific risks are fully covered.

The second step is the scenario assessment. For each scenario generated the banks estimate the potential frequency and loss severity. The assessment process is based on the expertise of subjects that have high competencies on OR and on information relevant to the scenario, such as historical losses, key risk indicators, industry experience and insurance coverage. It is obvious that the importance of the different types of information depends especially on the quality of the historical data available and its relevance to the current scenario assessment. Therefore, if the historical data are of poor quality or if the business is undergoing significant changes, such data cannot be used as basis for the estimate.

The third step concerns the validity of the data resulting from scenario assessment. This data, which will be used for risk capital modelling, must be of good quality and reflect the actual OR profile. Therefore, all under/overestimates of frequency/severity must be adjusted. There are multiple techniques used for this purpose: as mentioned above, the "two pairs of eyes principle", internal audit of the risk assessment process, comparison between actual losses and experts' expectations, comparison of the outcome of scenario assessments against internal audit findings, and challenge by group functions such as risk.

Once the quality of the scenario assessment data has been confirmed, these data can be used to obtain parameter values to be employed in the model for distributions or analytical solutions. This represents the fourth step of the approach, in which at least mean and standard deviation both for frequency and for severity are usually determined.

In the fifth step the determined parameters are fed into the risk model. The usual models employ a Monte Carlo simulation to compound all individual distributions per scenario class and organizational part into an overall aggregated potential loss distribution. Analytical models may be used alternatively.

Finally, the sixth step consists in drawing from the overall loss distribution values the output of the risk capital model: the economic capital or the regulatory capital. This makes it necessary to define the quantile in which we are interested, which is the absolute value corresponding to a given percentile.

In BCBS (2011), some critical considerations emerge on the use of SBA. In particular, the observation of the SBA models used in banking operations highlights the critical issues connected to the process of quantification/estimation. BCBS (2011) lists the following drawbacks:

- many SBA models do not apply statistical inference to raw scenario data. Very often the SBA model curves are predetermined and the scenario data are used only to estimate the parameters of those distributions (usually by percentile matching);
- banks generally use the same curve (usually the lognormal) to model the severity of the scenario data across all ORCs,[4] regardless of its business, size and complexity. The selection of a single curve across ORCs implies that the only admissible driver of variation in the operational risk exposure lies in the scenario-driven parameter estimates of the chosen distribution;
- a bank should ensure that the loss distribution(s) chosen to model scenario analysis estimates adequately represent the risk profile of the ORCs. In doing so, banks should also consider the potential differences with an LDA in terms of level of granularity[5] and dependence across the ORCs.

6.4 Conclusions

As we have seen in the previous pages, the LDA models lead to a robust and valid estimate of OR exposure, although they present a number of problematic issues that could be solved more suitably by resorting to the SBA methods. On the other hand, these latter methods offer greater flexibility, despite featuring some difficulties in justifying and ensuring accuracy of the results. Below we compare the two models, with the aim of evidencing their main principal potentials and limits (Bazzarello and Piacenza 2009).

As previously stated, the objectivity and exhaustiveness of the loss data certainly represent a point of strength of the LDA models, since the data can be easily reconciled with accounting information that can also be checked over time by the auditors and by the supervisory bodies.

This means that the input of the calculation model is neither information generated by the Operational Risk Management function nor a subjective estimate, as it can be found directly in the books of account. The SBA models generally refer to subjective judgements or estimated impacts, thus requiring greater efforts to check and justify the input data and therefore greater difficulties of validation.

The loss data of a bank can be integrated with external data. This combination may constitute the input for an LDA calculation model, thus improving the accuracy and sturdiness of the results with respect to the use only of the internal data.

Variations of the structure of the loss data over time are guided by the books of account, allowing the operational risk manager to take a clear and independent position of control in addition to showing management directly the impact of the dataset changes on the results of risk capital, allowing a clear identification of the intervention plans. The adjustments and the analyses of the historical series of loss data can be traced and directly connected to the processes and to the business. Loss data feeding can be partly semi-automated, by using procedures already available in the bank.

For all these reasons, the LDAs could represent an appropriate and favourable solution, with particular regard to the activities of review of the audit and of the supervisory authorities, of internal and external benchmarking, as well as justification of the results.

Moreover, the LDAs prove to be particularly rigid when it is necessary to obtain measures of risk referred to individual companies, products or processes in the case in which the availability of internal and external data related to these entities is very limited. In fact, risk capital calculated on a stand-alone basis using the LDAs is robust and accurate only when the numerous samples of the time series are statistically sufficient. Generally, the SBAs should prove to be better than the LDAs at providing consistent results for individual companies or business units. The SBAs offer the advantage of being flexible: they can be applied at different levels (at the organizational, divisional, location, new product, or even transactional) (Laycock 2014).

The SBAs are forward-looking and for this reason well suited to a dynamic business and organizational environment and support a

proactive risk management culture. In other words, "what-if" questions asked in a scenario analysis shift the focus of risk assessment to the future: scenarios outline pictures of the future or plausible explanations on possible "futures" (OeNB and FMA 2006). It follows that the SBAs immediately incorporate the changes occurred in the organizational environment. Accordingly also other key factors are more rapidly incorported in the estimates, such as organizational variations, strategy changes, different business activities, changes in the external context, improvement of controls, etc. On the other hand, LDA models mainly use past information, such as internal and external losses. In other words, they are backward-looking and the factors mentioned above are considered only when the relative historical series fall within the input of the model.

Using the SBAs makes it possible to consider the specific nature of the business, since the scenarios can be applied to any particular activity of the financial institution. Therefore, they allow greater granularity, since the models based on loss data require a significant amount of data in order to obtain sufficiently accurate estimates.

The models based on the scenarios can support, better than the LDAs, the dissemination and progress of the culture on operational risks. Indeed, the correct implementation of an SBA requires the constant support of experts who should be connected to all the key points of the organizational structure. In order to provide regular risk assessments, experts need in any case gather as much information as possible, keeping it constantly up to date. In addition, the evaluation and analysis of the risk factors and controls associated with the scenarios provide important information on how to improve OR management. It is obvious that once these improvements have been achieved and the OR profile of the organizational parts has decreased, the scenarios can be newly assessed.

The LDA models may sometimes present problems in terms of transparency of the results from the point of view of the business units. In fact, if sufficient training activity is not performed to explain the way in which the approach works and what are the major levers influencing the results, the LDA model could be seen as a true black box. This should not happen for the SBAs, since the risk measures for a certain business unit are referred directly to the estimates provided by such unit.

Owing to the many above-mentioned pros and cons of LDA and SBA approach, it is not possible to indicate which of the two is best in absolute terms. Accordingly, the best suggestion might be to adopt an approach that considers both loss data and the experts' assessments. It must, however, be reminded that the LDA type models have been used for decades in insurance practice with satisfactory results and, consequently, they may constitute a valid starting point for the implementation of a model meeting the AMA requirements.

Notes

1. The IMA requires classification of banking activities in specific BLs, each corresponding to a range of risk events. For each match business unit-risk factors is given an exposure indicator, which indicates the amount of events (Exposure Indicator—EI); internal loss data are then used to calculate the probability of the loss event, which indicates the frequency of the event (Probability of Loss Event—PE), as well as the loss deriving from the occurrence of the event, which equals its severity (Loss Given Event—LGE). The product of such entities expresses the expected loss that—for the determination of the partial capital requirement—must be multiplied by the factor γ that depends on the type of OR; the sum of the results for all the matches BL-risk factors determines the total amount of the OR regulatory capital. Obviously the IMA is based on the dependency between the unexpected and the expected loss by means of multiplying factor γ.
2. The SA is built on the preventive definition of total regulatory capital for OR, on the spreading of the OR own funds among the several BLs, and on the adjustment of the individual attributions according to the information provided by the indicators that inform both on the true operational risk exposure and on the quality and effectiveness of the control over each BL.
3. In order to minimize these biases, an institution must apply a number of bias mitigation techniques. Among these, the use of external data can help overcome the availability bias in identifying relevant scenarios. Besides, the provision of external frequency and impact statistics can act as an anchor for the participants' estimates.

4. ORC is the acronym of Operational Risk Category. ORC is defined by BCBS (2011) as "the level (for example, organizational unit, operational loss event type, risk category, etc.) at which the bank's quantification model generates a separate distribution for estimating potential operational losses. This term identifies a category of operational risk that is homogeneous in terms of the risks covered and the data available to analyze those risks."
5. Granularity is connected with the number of ORCs used within the model. BCBS (2011) points out that "There is currently a great variation both in the choice and the number of ORCs used by banks".

References

Aas, K. 2004. Modeling the dependence structure of financial assets: A survey of four copulas. Note, Norwegian Computing Centre, December.

Abdymomunov, A., and F. Curti. 2016. Improving the robustness of operational risk estimation and stress testing through external data scaling, April. http://ssrn.com/abstract=2622175.

AG (Advanced Measurement Approaches Group). 2012. Scenario analysis: Part 2: Practices. *Industry Position Paper*.

Aue, F., and M. Kalkbrener. 2007. LDA at work: Deutsche Bank's approach to quantifying operational risk. *Journal of Operational Risk* 1 (4).

Babbel, D.F., and K. Dutta. 2012. Scenario analysis in the measurement of operational risk capital: A change of measure approach. http://www.crai.com/publication/scenario-analysis-measurement-operational-risk-capital-change-measure-approach.

Bazzarello, D., and F. Piacenza. 2009. Il loss distribution approach e lo scenario based approach nell'esperienza UniCredit. In *Il Rischio operativo nelle banche italiane*, ed. G. Birindelli and P. Ferretti. Modelli, gestione e disclosure, Bancaria Editrice, Roma.

BCBS (Basel Committee on Banking Supervision). 2009. Observed range of practice in key elements of Advanced Measurement Approaches (AMA), July.

BCBS (Basel Committee on Banking Supervision). 2011. Operational risk—supervisory guidelines for the Advanced Measurement Approaches, June.

BIS (Bank for International Settlements)-Committee on the Global Financial System. 2005. Stress testing at major financial institutions: Survey results and practice, Basel.

Burt, G., G. Wright, R. Bradfield, G. Cairns, and Heijden K. Vander. 2006. The role of scenario planning in exploring the environment in view of the limitations of PEST and its derivatives. *International Studies of Management and Organization* 36: 50–76.

Chaudhary, D. 2014. Sensitivity analysis of scenario models for operational risk Advanced Measurement Approach. http://mpra.ub.uni-muenchen.de/60996/. MPRA Paper No. 60996.

Chapelle, A., Y. Crama, G. Hubner, and J.P. Peters. 2004. Basel II and Operational Risk: Implications for risk measurement and management in the financial sector, National Bank of Belgium, Working Paper.

Chernobai, A.S., R. Svetlozar, and F.J. Fabozzi. 2005. Composite goodness-of-fit test for left truncated loss samples, Working Paper.

Chernobai, A.S., S.T. Rachev, and F.J. Fabozzi. 2007. Operational risk: A guide to Basel II capital requirements, models and analysis. Willey.

Clemen, R., and C. Fox. 2005. Subjective probability assessment in decision analysis: Partition dependence and bias toward the ignorance prior. *Management Science* 51 (9): 1417–1432.

Demarta, S., and A.J. McNeil. 2005. The t copula and related copulas. *International Statistic Review* 73 (1).

Dutta, K., and J. Perry. 2013. A Tale of Tails: An empirical analysis of loss distribution models for estimating operational risk capital. Working Paper, Federal Reserve Bank of Boston, No. 6.

Embrechts, P. 2000. *Extremes and integrated risk management*. Risk Books.

Gregoriou, G.N. 2009. *Operational risk toward Basel III*. Wiley Finance.

Guray Uner, S. 2008. Loss distribution approach for the operational risk economic capital. SAS Global Forum, Paper 163.

Hosking, J.R.M., and J.R. Wallis. 1987. Parameter and quantile estimation for the generalized Pareto distribution. *Technometrics* 29 (3).

Jenkinson, D. 2005. The Elicitation of probabilities—a review of the statistical literature', Bayesian Elicitation of Experts' Probabilities (BEEP). Working Paper, University of Sheffield, U.K.

Kahneman, D., and A. Tversky. 1974. Judgement under Uncertainty: Heuristics and biases. *Science* 185: 1124–1131. September.

Laycock, M. 2014. Operational risk quantification: Scenarios. Thomson Reuters Accelus, September.

Lemmi Gigli, N. 2005. Trasferimento del Rischio Operativo. V Convention Aifirm, Convegno Nazionale Risk Management, Ottobre 20–21.

Lubbe, J., and F. Snyman. 2010. The advanced measurement approach for banks. *IFC Bulletin*, (33), 141–149.

McNeil, A.J., R. Frey, and P. Embrechts. 2005. Quantitative risk management. Princeton series in Finance.

Mignola, G., and R. Ugoccioni. 2005. Tests of extreme value theory. *Operational Risk* 6 (10).

Moscadelli, M. 2004. The modelling of operational risk experience with the analysis of the data collected by the Basel Committee. Banca d'Italia, Temi di discussione, n. 517.

Oakley, J., and A. O'Hagan. 2004. Probability is perfect, but we can't elicit it perfectly. *Reliability Engineering and System Safety* 85: 239–248.

OeNB (Oesterreichische Nationalbank), FMA (Austrian Financial Market Authority). 2006. Guidelines on Operational Risk Management.

Rippel, M., and P. Teplý. 2008. Operational Risk—Scenario Analysis, Institute of Economic Studies, Faculty of Social Sciences. Charles University in Prague, IES Working Paper, No 15.

Romano, C. 2002. Calibrating and simulating copula functions: An application to the Italian stock market. Working Paper, 12, Cidem.

Romano, C., and A. Di Clemente. 2003. A copula extreme value theory approach for modeling operational risk. Working Paper.

Savelli, N. 2005. L'approccio attuariale nella valutazione del rischio operativo: il Loss Distribution Approach e l'Extreme Value Theory. Corso di aggiornamento ASSBB—Università Cattolica su Il rischio operativo nelle banche: metodologie di valutazione e strumenti di copertura assicurativa, Milano, 7–8 Giugno.

sbAMA (The scenario-based AMA) (sbAMA) working group (2003) "Scenario-based AMA", May.

Segal, S. 2011. *Corporate value of enterprise risk management.* Wiley.

Shih, J., A. Samad-Khan, and P. Medapa. 2000. Is the size of an operational loss related to firm size? *Operational Risk* January.

Sklar, A. 1959. Fonctions de repartition à n dimensions et leurs marges. Institute de Statistique de l'Université de Paris.

Spetzler, C., and C.S. Von Holstein. 1975. Probability encoding in decision analysis. *Management Science* 22 (3): 340–357, November.

Torresetti, R., and C. Nordio. 2014. Scaling operational loss data and its systemic risk implications, February. http://ssrn.com/abstract=2360483.

Watchorn, E. 2007. Applying a structured approach to operational risk scenario analysis in Australia. Information Paper, Australian Prudential Regulation Authority, September.

7

Operational Risk: Evidence from Italian Cooperative Banks

7.1 Introduction

In the case of the small banks, operational risk management generally takes on a secondary role compared to other risks, more closely associated with typical banking activity (in primis credit risk). This can be mainly due to the low degree of diversification of the activities carried out by smaller banks, which decreases the operational risk exposure and consequently the need to employ human, financial and technological resources in sophisticated systems of operational risk management.

In this chapter we present the results of a survey on a sample of Italian cooperative banks. The survey explores different research areas: organizational aspects, measurement methods, Second Pillar, insurance coverage, and trade associations/outsourcing.

7.2 OR Management in Smaller Banks

In the setting of smaller banks with a more traditional business, OR management takes on a secondary role compared to the management of other risks that are more closely associated with typical banking activity,

G. Birindelli and P. Ferretti, *Operational Risk Management in Banks*,
Palgrave Macmillan Studies in Banking and Financial Institutions,
DOI 10.1057/978-1-137-59452-5_7

such as—first and foremost—credit risk. This can be mainly due to the low degree of diversification of the activities carried out by smaller banks, which decreases the OR exposure and consequently the need to employ human, financial and technological resources in sophisticated systems of operational risk management.

Such considerations also explain the choice towards less evolved methods in the calculation of OR capital requirement, as evidenced by the results of the QIS-5 (Quantitative Impact Study 5), which show a widespread adoption, at international level, of the basic and standardized approaches among banks featuring less complex organization (Table 7.1).[1]

In general, the trend towards adopting more simplified approaches is justified by the operational and market characteristics featured by smaller banks, which inevitably restrain OR management and measurement from being developed to their full potential. There are, however, few smaller banks willing to undertake a more efficient OR management in view of benefits in terms of control and cutting down on operational risk.

7.3 Overall Results of the Survey

A recent survey of ours on a sample of cooperative banks (in Italian, banche di credito cooperativo—BCCs)[2] has investigated the state of the art of OR management on behalf of smaller banks (Birindelli and Ferretti 2009). In order to capture the attitudes smaller banks have

Table 7.1 Types of OR approaches by level of diffusion among banks. *Source* BCBS (2006)

Approach	Group 1 Banks	Group 2 Banks
Basic indicator approach	2	81
Standardized approach	32	65
Advanced measurement approach	22	0
Total	56	146

Note The figures in this table include banks of G-10 countries with the exception of US. G-10 countries are: Belgium, Canada, France, Germany, Italy, Japan, Luxembourg, the Netherlands, Spain, Sweden, Switzerland, the United Kingdom and the United States

towards OR and the many observation points (organization structure, measurement methods, market disclosure, and so on), we purposely selected a sample of BCCs that could help us understand the main issues linked to small company size. Our sample selection focused on those BCCs having headquarters in Tuscany (Italy) and featuring a set of characteristics representative of the cooperative banking system.

The BCCs were first asked to provide some information on their company profile, and were then invited to complete a 5-section questionnaire (see Appendix) enquiring on (i) organizational aspects, (ii) measurement methods, (iii) Second Pillar, (iv) insurance coverage, (v) and trade associations/outsourcing. Participation was low, reaching approximately 50%. In most cases banks declined our invitation claiming that their extremely small size and their exclusive use of the basic approach would not have contributed to our study.

The sample, which was initially composed of 19 respondents, was later expanded by adding four banks associated with the Federation of Lazio Umbria Sardegna (Federlus). Below, data on the size of participating banks are summarized in terms of total assets and regulatory capital (Table 7.2), whereas the complete list of banks is provided at the end of the chapter.

Interestingly, the persons (within the participating institutions) most often assigned to complete the questionnaire were risk controllers, who were in many cases already assigned to other responsibilities such as in the control area, planning and control, and compliance.

In the following sections we report the results on the information obtained in response to the questionnaire, distinguishing between banks with headquarters in Tuscany from those associated with Federlus.

Table 7.2 Size of BCCs participating to the survey—values in thousands of euros (own processing)

	Min	Max	Mean	Median
BCCs in Tuscany				
Total assets	27,281	3,801,622	600,696	379,475
Regulatory capital	4,168	209,205	47,828	37,358
Federlus BCCs				
Total assets	43,000	477,010	209,706	159,407
Regulatory capital	3,800	33,448	15,942	13,260

7.3.1 Organizational Aspects

BCCs in Tuscany

42.1% of BCCs in Tuscany had a specific function dedicated to OR management, whereas the others either did not have a specific organizational control unit (26.3%) or the OR was directly managed by the officer in charge of the organizational unit where the risk had its source (31.6%). As expected, none of the banks had an OR committee. In many cases the OR function corresponded to the risk controller, who (as mentioned above) at the same time covered other roles (e.g., internal compliance manager, officer in charge of managing other types of risks). According to the open comments and notes the respondents gave in the questionnaire, it appears that this function also performed second level controls, while a third level for OR controls was assigned to an Inspection Unit/Control Area.

Where available, the function was organizationally placed as a staff function reporting to the general manager (6 banks), under the board of directors (1 bank) and within the planning and control (again, 1 bank).

The tasks/responsibilities assigned to the personnel involved in the performance of the function's activities (whose number never exceeds 1) were always formalized. The instruments adopted in this regard were mostly regulations approved by the board of directors and related implementation regulations; participants also mentioned specific job descriptions, service orders, checks plans, Internal Capital Adequacy Assessment Process (ICAAP) regulations and internal communications.

The function's degree of responsibility, which was evaluated on a range from 1 to 5, was distributed quite uniformly among the activities listed in the questionnaire and reported in Table 7.3, with a maximum mean score (3.4) reached for advice to the board of directors and the top management, and lowest mean score (3.0) for the assessment of OR exposure in the case of entering new markets and/or offer of new products, as well as for the definition of tolerance thresholds for the business units.

The same range was used to enquire on the degree of involvement in OR management on behalf of specific functions: OR function/unit, Risk Management (RM), Internal Audit (IA), legal, compliance,

the individual business units, units delegated to the management of information-accounting systems, planning and control, and organization. The degree of involvement, calculated as the average of the values reported in the questionnaires, generally had values greater than 3, with a minimum value for the planning and control and a maximum for the RM (see Table 7.4).

Table 7.3 Responsibility score attributed to the OR function—BCCs in Tuscany (own processing)

Task	Mean
Defining OR management policies	3.2
Developing OR measurement methods	3.2
Checking the implementation of such methods and reviewing them periodically	3.2
Disseminating OR culture by promoting awareness raising	3.2
Contributing to the assessment of OR exposure in the event of entering new segments of the market and/or offering of new products	3.0
Advising the board of directors and the top management in defining the limits of controls and the delegation of powers	3.4
Monitoring the loss data collection	3.1
Establishing OR tolerance thresholds for the business units	3.0

Note Each score corresponds to a degree of responsibility: 1 = not accountable; 2 = slightly accountable; 3 = quite accountable; 4 = mostly accountable; 5 = completely accountable

Table 7.4 Engagement in OR management—BCCs in Tuscany (own processing)

Function/Unit	Mean
OR function/unit	3.6
Risk management	3.7
Internal audit	3.3
Legal	2.6
Compliance	3.4
Individual business units	3.0
Units assigned to management of information-accounting systems	2.7
Planning and control	2.3
Organization	3.1

Note The mean score for the OR function/unit is obtained by considering only those banks having a function/unit ad hoc; the other scores instead consider all 19 banks in Tuscany. The scores range from 1 to 5: 1 = function not engaged; 2 = function with little engagement; 3 = function sufficiently engaged; 4 = function very engaged; 5 = function totally engaged

As described by participating banks, the main tasks/skills in OR management are identified in the following:

- RM: mapping/identification of the OR; risk measurement and statistical analysis related to the quantification of OR; continuous monitoring; drafting work processes for limiting underlying OR; preparation of reports on the OR; advising on definition of control limits and on the delegation of powers; evaluation of the OR in the case of offer of new products; determination of the maximum risk exposure; assessment of the adequacy and proper functioning of the endogenous risk factors (processes, information-accounting systems, human resources); definition of the strategies for OR mitigation;
- IA (outsourced in 17 cases): assessing process adequacy, effectiveness of controls and of OR mitigation strategies; supporting RM for the census of the risks; reviewing the work of the RM; reporting to top management on any undetected OR and the malfunctioning of control units and/or their monitoring. In many cases banks reported also the monitoring on the legitimacy of changes to the authorization procedures for accessing the information system with the aim of improving segregation among functional units, and the monitoring on employee operations by introducing appropriate IT system locks;
- Legal function: supporting RM for the identification and assessment of legal risks; detecting and managing complaints received from customers; identifying damages to reputation resulting from the occurrence of OR; monitoring of indicators such as the number and amount of losses due to internal and external frauds, disputes, insurance compensations due to external causes, revocatory actions, and robberies;
- Compliance (also this function is outsourced in 17 banks): monitoring of compliance of contracts and internal regulations; advising RM for the identification and assessment of risks; ex-ante controlling on processes; contributing to the diffusion of OR culture at business unit level; defining work processes in collaboration with the organization;
- Planning and control: estimating losses on various market segments and products specified in the strategic and operational plan; measuring the OR within the ICAAP; transferring RM dispositions into the annual and strategic plans;

- Organization: drafting of work processes and their modification to mitigate the OR; verification of the correct distribution of processes among the personnel; support to the RM for verification of operational and IT procedures and of related controls to protect employee safety; preparation of internal regulations for OR management.

The descriptions listed above evidence that some tasks were assigned to different functions; nevertheless, the division of roles appears mostly uniform across the different banks.

The last questions on organization address reporting; in particular, they are related to the person assigned to drafting reports on OR, to the frequency of the reports and to their recipients. Aside from two banks that had still not done that, in the remaining banks this task was generally assigned to the risk controlling unit, that prepared the reports sometimes in concert with other functions (namely, IA and general manager). Only in two cases the preparation of the reports was done by different parties: the internal audit in one bank, and the staff from planning and control function in the other bank. The frequency of reports was once every three/four months in most cases, and every six or twelve months in a few banks. Among the recipients of the reports, all survey respondents mentioned the board of directors, supported in some cases by general managers, the managers responsible for business units, the audit committee and the board of auditors.

Federlus BCCs

Among the four Federlus BCCs, three banks did not have a dedicated OR function/unit, while the remaining bank had a risk control service that was assigned to other risks, in addition to OR. Also these banks had considered the risk controller—or analogous figure—as an organizational control unit that was not specifically assigned to OR management, probably due to the concomitant assignment of responsibilities in monitoring several risks.

The risk control service, which operates as a staff unit reporting to the general manager and has two units of personnel, was formally assigned

to specific tasks as expressed in the internal regulations and was totally accountable for all the tasks listed in Table 7.3.

The degree of involvement of different functions assigned to OR management (Table 7.5) was visibly lower compared to that of BCCs in Tuscany (Table 7.4).

In that bank with an ad hoc function, RM performed all the activities listed in Table 7.3, alongside monitoring the other risks as well; the remaining banks reported among their main tasks: checking for any operational irregularities that could generate OR, drafting of reports on mitigation, capital requirements, effectiveness of insurance contracts and on the adequacy of processes and procedures. As in reference to the IA (outsourced in all cases), the answers point towards the assessment of business processes that could have generated OR and the drafting of OR reports. Similar replies were also found in reference to compliance (this, too, was outsourced in all four banks), responsible for the analysis and assessment of the strategic risk and for the supervision of the conformity of the processes. Only one bank reported the involvement of the legal function—which exerted the skills in the field of legal risk and litigation procedures—while another bank reported the involvement of planning and control—which was also responsible for the assessment of the legal risk and associated reputational risk. Finally, organization managed and supervised the decision tables of the information system, established business processes and operated on them, and was responsible for designing and updating of the business continuity plan.

Table 7.5 Engagement in OR management—Federlus BCCs (own processing)

Function/Unit	Mean
OR function/unit	5.0
Risk management	3.5
Internal audit	2.7
Legal	1.2
Compliance	1.7
Individual business units	3.0
Units assigned to management of information-accounting systems	1.7
Planning and control	1.2
Organization	2.0

Note The scores range from 1 to 5: 1 = function not engaged; 2 = function with little engagement; 3 = function sufficiently engaged; 4 = function very engaged; 5 = function totally engaged

Reporting was active in three banks: in all cases, there was similarity in terms of the structure carrying out the reporting (risk control service/risk controller), and of frequency in issuing the reports (in all cases, every three/four months). The recipients were in two cases the board of directors, and in the other case was the general manager.

7.3.2 Measurement Methods

BCCs in Tuscany

The overall results from the survey evidenced that all Tuscan banks adopted the basic indicator approach, and only one of them was moving (in the short-medium term) towards more advanced approaches for regulatory purposes. The adoption of the BIA was most often justified by the banks' small size and the benefits expected from more sophisticated methods, which (according to responses) appeared too exiguous to counterbalance the high investments in human resources and IT systems, needed for the implementation of the other methods (standardized approach and, all the more, advanced measurement approach). Banks also believed that the use of less sophisticated approach was consistent with their actual risk profile. Other reasons can be ascribed to the need of sharing the adoption of more advanced approaches with the associative structures of the cooperative system.

Differently, five banks had adopted for management purposes a more sophisticated approach than that used for the calculation of the regulatory requirement, with greater attention towards internal loss data, business environment and internal control factors, and Key Risk Indicators (KRIs). In particular, responses to the question on the frequency of use of the elements/tools for the estimation of the risk exposure provided the mean values reported in Table 7.6.

Specifically, the KRIs—used in 11 BCCs—were (according to the replies to multiple-choice question):

- total cash shortages;
- number of documents non-compliant with regulations;
- inconsistencies identified upon IA inspections;

Table 7.6 Frequency of use of tools for OR assessment—BCCs in Tuscany (own processing)

Elements/Analyses	Mean
Risk maps and process charts	2.2
KRIs	2.4
Internal data	2.7
External data	1.2
Scenario analysis	1.6
Business environment and internal control factors	2.5

Note The scores ranging from 1 to 5 indicate: 1 = never used; 2 = used in less than 25% of cases; 3 = used in number of cases between 25% and 50%; 4 = used between 50% and 75% of cases; 5 = used in more than 75% cases

- number of manual errors;
- other indicators: complaints, litigation procedures and losses in lawsuits, labour compensations, thefts and robberies, insurance compensations, inconsistencies identified by compliance (all of which were reported from the same respondent bank).

The internal loss data are reported separately in 13 banks when data take on the nature of credit/market risk boundary losses.

The limited resort to external data (in five BCCs) did not involve the use of scaling techniques in any case, either for the frequency, or the severity, or the integration with internal losses to build a single distribution of frequency and severity.

In those cases in which scenario analysis was performed (five banks) (according to the answers to this multiple-choice question), the analysis aimed at collecting information on:

- probability and severity;
- average value of loss;
- worst case scenario;
- ORs embedded in processes and products;
- quality of internal controls.

In a setting in which a formalized method for scenario construction was lacking, those assigned to structuring the questionnaire in order to carry

out this analysis were: OR control unit, the risk manager/risk controller, the manager responsible for the business continuity plan, the risk controlling and compliance service. The questionnaire addressees were mainly managers responsible for business units and, in one case, the board of directors.

The assessment of business environment and internal control factors was found in 10 banks and mainly involved: IA, OR control unit, the manager responsible for business units, organization, inspection unit, risk manager/risk controller, general manager, personnel working in planning and control.

Despite the elaboration of subjective estimates—although, with a negligible weight—none of the banks had implemented a system for verifying the reliability of such estimates, such as cross-checks between true losses and estimated expected losses, and between evaluations by the managers responsible for business units and those by internal auditors.

In all cases the findings evidenced an OR management still at its early design stage and capable of being further developed with the help of the associative structures of the cooperative system.

Federlus BCCs

Similar results have been found for the Federlus BCCs which reported the BIA as the only method being adopted, and none manifested any intention to change towards more sophisticated approaches (nor in the short or medium term), owing to the same size-related reasons (high costs and need of difficult-to-find resources due to the small size of the BCCs).

Also for these BCCs the frequency of use of elements and tools for evaluating the risk exposure was low: as can be seen by comparing data in Tables 7.6 and 7.7, the mean rates were always lower for the Federlus BCCs and the use of risk maps and process charts, as well as internal loss data, was actually inexistent.

The KRIs, used by two banks, were represented by irregularities identified by the IA and cash shortages; internal loss data (when connected to credit and market risk), were reported separately in two cases.

Table 7.7 Frequency of use of tools for OR assessment—Federlus BCCs (own processing)

Elements/Analyses	Mean value
Risk maps and process charts	1.0
KRIs	1.5
Internal data	1.0
External data	1.1
Scenario analysis	1.2
Business environment and internal control factors	1.2

Note The scores ranging from 1 to 5 indicate: 1 = never used; 2 = used in less than 25% of cases; 3 = used in a number of cases between 25% and 50%; 4 = used between 50% and 75% of cases; 5 = used in more than 75% cases

As to external data, the results were as for the Tuscan BCCs: the only bank that had resorted to their use had not adopted scaling techniques nor integration with internal losses.

Only one bank conducted the scenario analysis and estimated the business environment and internal control factors: as to the former the self-assessment was intended exclusively to evaluate the quality of internal controls; as to the latter, estimation was conducted mainly on the basis of the findings of the Federlus audit analysis. Finally, the bank did not check the reliability of subjective data.

7.3.3 Operational Risk in the Second Pillar

BCCs in Tuscany

This section focuses on the calculation model for economic capital, which was found in five BCCs in Tuscany and in two banks under planning. None of the banks that had not adopted a model was working to establish one.

The model was defined by RM, which in one case relied on a service agency within the BCC network and on external professionals, whereas the model was defined by the board of directors only in one bank.

As commented by the participants, the most frequently measured risks were credit, market and operational risks. The model included OR

in four banks. Its incidence (expressed in percentage and in one case as absolute value) was 4.5, 7.4, 15% respectively and 2.147 millions of euros.

In few cases the model took into account the benefits from diversification, namely diversification among types of risk, though without distinction among different business units.

The reasons that led to the implementation of an economic capital model (Table 7.8) were mainly linked to the compliance with regulatory requirements, followed by the willingness to improve strategic planning and define risk limits.

Among the respondents, the economic capital measures were mainly used to assess/allocate the capital; in one case they were also used for the evaluation of the profit margin for each product/service and the profit margin at customer level.

The indicators that correlate banking performance to the level of risk were used by eight banks and were at the planning stage in two others. All 10 BCCs signalled the (ongoing or planned) joint use of the following indicators: RAROC (Risk-Adjusted Return on Capital), RORAC (Return on Risk-Adjusted Capital), and RARORAC (Risk-Adjusted Return on Risk-Adjusted Capital). EVA (Economic Value Added) was reported by eight banks and EaR (Earning at Risk) by four.

The main objectives for the use of such indicators claimed by the banks were an efficient capital allocation (nine banks) and the assessment of the results achieved compared to those planned (six banks);

Table 7.8 Reasons relevant for calculation of economic capital—mean values for BCCs in Tuscany (own processing)

Reasons	Relevance
Regulatory requirements	4.6
Improvement of strategic planning	3.4
Definition of risk appetite	2.2
Improvement of rating	1.4
Improvement of pricing	2.4
Definition of risk limits/capital allocation	3.4
Assessment of risk-adjusted performance	2.0

Note The scale ranges from 1 to 5: 1 = non relevant; 2 = little relevant; 3 = quite relevant; 4 = very relevant; 5 = extremely relevant

following in order, was the comparison of performance between the different business units (two banks), while the last option listed in the multiple-choice answer (the establishment of a system of incentives linked to risk) had not been reported by any of the banks.

Federlus BCCs

Only one of the Federlus BCCs had in place a model for calculating economical capital. The model encompassed OR—the incidence of which summed up to two hundred thousand euros—but did not take into account the benefits deriving from diversification.

As to risk indicators, none of the Federlus BCCs used any. However, after the survey some Federlus banks verified the capital sustainability of their own strategic plans, quantifying the RORAC for each projection period.

7.3.4 Insurance Coverage

BCCs in Tuscany

This section of the survey opens enquiring on whether the bank had implemented a comparison between insurance contracts and events causing an OR loss: six BCCs in Tuscany had already acted in this direction and half of these had been pushed to review the insurance contracts in terms of their change and/or their renegotiation.

The management of insurance policies was assigned to several organizational areas and in some banks even to more units/managers, among which: the general manager (5 cases), the OR function (4 cases), purchasing and logistics (2), legal (2), organization (2), administration (2), human resources (1).

The traditional forms of insurance coverage were never accompanied by innovating forms of insurance.

Federlus BCCs

The comparison between insurance contracts and events causing an OR loss found scarce diffusion also among the Federlus BCCs: only one bank had performed the comparison and had revised the insurance contracts accordingly. The organization units that were involved in the management of insurance contracts were represented by risk management, organization and management control.

As for the BCCs in Tuscany, none of the Federlus banks had resorted to more innovating forms of insurance.

7.3.5 Trade Associations and Outsourcing

BCCs in Tuscany

The opening part of the section addresses the tasks performed by trade associations and networks of BCCs supporting OR management for individual banks.

Despite all—except two[3]—of the BCCs in Tuscany belonging to the Tuscan Federation, the participating intermediaries provided dis-homogeneous replies: while six banks did not mention any support on behalf of the Federation, the remaining 11 listed a number of tasks performed by the Federation towards a better OR management; although it was emphasized that such tasks referred to evolving projects thus would have yielded returns in the coming years.

In general, the responses pointed to a number of actions gathered within the Federation, spanning from support in the loss data collection (with the intention of creating a regional database), to the definition of KRIs, to the future implementation of more advanced methods than the BIA, to elaboration of economic capital models, to the spreading of information under the Third Pillar, to the closing of insurance contracts. Conversely, there was less support—either actual or

expected—from the network: only one bank benefiting from tasks performed by Cabel.[4] Among the services received by the respondent bank were the production of management software and the management and strategic advice.

The section closes with an enquiry on any outsourcing of phases in OR management. Eighteen banks had relied on outsourcing, and almost all had turned to the local regional Federation.[5] The phases derived from the outsourcing of IA and compliance and thus concerned the support tasks described in Sect. 7.3.1 on organization.

Federlus BCCs

Some divergences in the appreciation of the support provided by the trade associations were also found among the Federlus BCCs: only two banks acknowledged support in OR management—especially in a long-term view—both in terms of implementation of KRIs and the preparation of the information under the Pillar III.

Findings evidenced a lack of support from the network of BCCs, while there were cases of outsourcing some phases of the OR management process. As for the Tuscan institutions, these were mainly audit and compliance tasks outsourced to the Federation.

7.4 Conclusions

The present survey provides some interesting insights: on the one hand, it evidences some differences among the BCCs in the different OR observation profiles proposed by the sections of the questionnaire; on the other, it evidences common trends and general issues to be addressed in the near future.

The analysis of the organizational structure indicates the widespread presence of a risk controller who appears to be in charge of monitoring operational risks, as well as of responsibilities and tasks in other areas; among such tasks, the appointment as internal compliance manager was most recurrent. The risk controller is also present in the institutions

that claim to lack an OR control unit: differently from the rationale followed by the other respondent banks in elaborating the answers, these do not recognize this figure as a subject with specific tasks of the OR management, likely because of the variety of additional tasks assigned to him/her.

A certain homogeneity can be recognized in the type of tasks performed by the functions that collaborate towards OR management, although there is much room for increasing involvement and developing synergies. This observation is justified in the light of the capital requirements quantification method followed (BIA), which did not certainly help the development of a sound organizational structure distinguished by a formalization of roles aiming to a joint and integrated OR management.

Indeed, all BCCs have adopted the BIA. However, the findings do highlight signs indicating a tendency towards a greater awareness in risk control and the use of tools of analysis to achieve this. In the future, banks will be required to keep more focus on the economic capital calculation models, not only to expand the range of measured risks and to refine the calculation of risks and the treatment of the benefits deriving from diversification, but also to integrate the models with the system of strategic and operational planning. It is likely that there will be an increased awareness on the benefits deriving from the use of more advanced methods (which to date are believed still to be inferior compared to the costs for implementation).

The path ahead is still long: the size of these banks, the availability of resources (human, financial and technological) and the level of specialization that can be achieved by these banks represent elements that hinder the achievement of an effective OR management.

The use of the BIA is also at the root of the few cases of revision of insurance contracts, for which the deduction in the calculation of capital requirements is not allowed.

Lastly, the responses evidence that there are expectations around support activities provided by local federations and by the centralized structures of the cooperative system. In the view of improving OR management mechanisms and self-assessment of the ORs in individual institutions, banks expect tasks be handled by cooperative associations

(assistance on the technical, procedural and organizational requirements required by prudential regulations). The support may extend to the loss data collection at the level of the entire BCC system, in which case the significance of the data would give a strong impetus to the use of different models from the BIA, also for management purposes alone.

List of Participating Banks

BCCs in Tuscany

Banca di Anghiari e Stia, Banca Apuana, Banca di Cambiano, Banca di Cascia di Reggello, Banca di Castagneto Carducci, Banca della Costa d'Argento, Banca di Impruneta, Banca di Montepulciano, Banca Monteriggioni, Banca del Mugello, Banca di Pescia, Banca di Pontassieve, Banca di Saturnia, Banca di Signa, Banca Versilia Lunigiana e Garfagnana, Banca di Vignole, Credito Cooperativo Area Pratese, Credito Cooperativo Fiorentino, Credito Cooperativo della Valdinievole.

Federlus BCCs

Cassa Rurale ed Artigiana dell'Agro Pontino, BCC della Tuscia, Banca di Formello e Trevignano Romano, BCC Privernate.

Notes

1. The Basel Committee on Banking Supervision (2006) breaks down banks into Group 1 or Group 2, with those in Group 1 fulfilling the criteria as stated: "the bank has a Tier 1 capital in excess of €3 billion; the bank is diversified; the bank is internationally active". Both classes of financial intermediaries belong to: "European countries which are either EU member states, EU accession candidates or members of the European Economic Area (EEA). In total this group comprises the

Committee of European Banking Supervisors (CEBS), which includes 30 countries (both G10 and non-G10), 20 of which provided data for QIS 5. Since they are all CEBS member or observer countries this group is referred to as the CEBS group".

2. For the definition of BCCs, we invite the reader to visit the website of the cooperative banking system (http://www.creditocooperativo.it/template/default.asp?i_menuID=42125): "The Credito Cooperativo is a system based on a network comprising 364 cooperative banks called Banche di Credito Cooperativo, Casse Rurali, and Casse Raiffeisen in Alto Adige; associative structures; and several service companies, all of which work together to guarantee a complete and diversified range of products, in keeping with the values and identity of a cooperative. The most important feature of these cooperative banks (BCCs) is that of being local, mutual, not-for-profit cooperatives." As to the associative structure, it "is subdivided into three levels: local (BCCs), regional (Local Federations) and national (Federcasse). The individual BCCs are associated with the Local Federations (representing one or more regions) which in turn are members of Federcasse, the Italian Federation of BCCs. Federcasse represents and protects the rights of its associate banks, offering them legal, fiscal, and organizational assistance, while providing support towards communications and training, so as to benefit the entire Credito Cooperativo system."
3. These were banks associated to the Associazione Generale Cooperative Italiane.
4. A support network for local banks established in 1985 thanks to the initiative of three Tuscan rural banks; the network provides services to many institutions among which several Italian subsidiaries of foreign banks.
5. Sixteen BCCs relied on the Federation's centralized structure both for IA and compliance, while only one bank relied on it for the compliance. One last bank had outsourced only the IA to another association. The outsourcing mainly concerned IT services and services related to the management of receipts and payments, and advanced technological support for a better interaction with the customers.

Appendix

Survey on Operational Risk Management

1. Bank's information

Name of the BCC: _____

Total assets: _____

Share capital: _____

Regulatory capital: _____

Role/position of the compiler within the bank: _____

2. Organizational aspects

2.1 From an organizational point of view, your bank:

Does not have a dedicated OR function ☐

Does have a dedicated OR function ☐

The OR is directly managed by the managers responsible for the unit in which it originated ☐

There is the OR committee within the board of directors ☐

Other (specify)_____

2.2 In the case there is a dedicated function, where is it located within the organization chart?

Under the board of directors ☐

As a staff function reporting to the general manager ☐

Within the planning and control function ☐

Within the IA ☐

As a staff function reporting to the managing director ☐

Other (specify) _____

2.3 In the case there is a dedicated function, how many personnel units are involved?

_____

2.4 In the case there is a dedicated function, has there been a formal assignment of tasks and responsibilities? If so, with which instruments (internal regulation and communication, non-official regulation, and so on)?

No, the assignment of tasks and responsibilities has not been made formal ☐

Yes, by means of _____

2.5 In the case there is a dedicated function, which is its degree of responsibility in carrying out the following tasks? (Scores range from1 to 5: 1 = not accountable; 2 = slightly accountable; 3 = quite accountable; 4 = mostly accountable; 5 = completely accountable)

	1	2	3	4	5
Defining OR management policies					
Developing OR measurement methods					
Checking the implementation of such methods and reviewing them periodically					
Disseminating OR culture by promoting awareness raising					
Contributing to the assessment of OR exposure in the event of entering new segments of the market and/or offering of new products					
Advising the board of directors and the top management in defining the limits of controls and the delegation of powers					
Monitoring the loss data collection					
Establishing OR tolerance thresholds for the business units					

2.6 Overall, which units/functions are engaged in OR management and to what degree? (Scores range from 1 to 5: 1 = function not engaged; 2 = function with little engagement; 3 = function sufficiently engaged; 4 = function very engaged; 5 = function totally engaged)

	1	2	3	4	5
Operational Risk function/unit					
Risk management					
Internal audit					
Legal					
Compliance					
Individual business units					
Units assigned to management of information-accounting systems					
Planning and Control					
Organization					
Other (specify)					

2.7 Describe the main tasks/skills in OR management for each function listed:

Risk management	
Internal audit	
Legal	
Compliance	
Planning and Control	
Organization	
Other (specify)	

2.8 Who drafts the OR report?

OR function ☐

Managers responsible for business units ☐

Other (specify)_____

2.9 How often are the reports prepared?

Monthly ☐

Every three/four months ☐

Every six months ☐

Yearly ☐

2.10 Who are the recipients of the report?

board of directors ☐

managing director ☐

Risk management committee ☐

OR function ☐

Planning and Control ☐

Managers responsible for business units ☐

Audit committee ☐

Other (specify)_____

Comments/details on section 2: _____

3. OR measurement methods

3.1 Which of the following methods do you use for regulatory purposes?

basic indicator approach ☐

standardized approach ☐

advanced measurement approach ☐

3.2 In the case BIA is used, do you plan to adopt more sophisticated approaches in the short medium term?

Yes ☐

No ☐

3.3 If not, why (specify)?

_____
_____
_____
_____

3.4 In the case BIA is used, is another more evolved approach used for internal purposes?

Yes ☐

No ☐

3.5 Which of the following instruments do you use most often to identify and measure OR exposure? (1 = never used; 2 = used in less than 25% of cases; 3 = used in number of cases between 25% and 50%; 4 = used between 50% and 75% of cases; 5 = used in more than 75% cases).

	1	2	3	4	5
Risk maps and process charts					
Key Risk Indicators (KRIs)					
Internal data					
External data					
Scenario analysis					
Business environment and internal control factors					

3.6 Are the losses linked to credit and market risk evidenced?

Yes ☐

No ☐

3.7 In the case you use key risk indicators, which ones do you use?

Number of manual errors ☐

Total cash shortages ☐

Number of documents non-compliant with regulations ☐

Inconsistencies identified upon IA inspections ☐

Other (specify)_____

3.8 In the event you resort to public or consortium databases, do you use any scaling techniques for frequency, severity, or for both?

No ☐

Yes, for frequency ☐

Yes, for severity ☐

Yes, for both ☐

3.9 Are the external data integrated with the internal ones towards the establishment of a single frequency and severity distribution?

Yes ☐

No ☐

3.10 If so, which approach do you use?

_____

3.11 In the event you use scenario analysis, which are the pieces of information collected?

Probability and severity ☐

Average value of loss ☐

Worst case scenario ☐

ORs embedded in processes and products ☐

Quality of internal controls ☐

Other (specify)_____

_____

_____

3.12 Who is assigned to structuring the questionnaire that will be used for conducting the scenario analysis?

_____
_____

3.13 Who are the addressees of the questionnaires?

_____

3.14 Is there a formalized method for building the scenarios in place?

Yes ☐

No ☐

3.15 In the case the business environment and internal control factors are evaluated, which is the organizational unit assigned to such evaluation?

_____

3.16 Are there in place any control mechanisms for subjective estimates?

Yes ☐

No ☐

3.17 If so, which are they?

Cross-checks between true losses and estimated expected losses ☐

Cross-checks between evaluations by the managers responsible for business units and those by Internal Auditors ☐

Other (specify)_____

_____

Comments/details on section 3:

_____

4. OR in the Second Pillar

4.1 Do you use a model for calculating the economic capital?

Yes ☐

No, but we are planning to adopt one ☐

No, and we are not planning to adopt one ☐

4.2 If you do use a model for calculating the economic capital, which function established it?

Risk management ☐

Planning and Control ☐

Other (specify) _____

4.3 If you do use a model for calculating the economic capital, is OR included? If so, which is its incidence in percentage?

No, it is not included ☐

Yes, it is included and its incidence is _____

4.4 If you do use a model for calculating the economic capital, does it take into account benefits deriving from diversification?

No ☐

Yes, it does include benefits deriving from diversification among the different types of risk ☐

Yes, it does include benefits deriving from diversification among the different business units ☐

Yes, it does include benefits deriving from diversification among risks and business units ☐

Other (specify)_____

4.5 In the case you do use models for calculating economic capital, which are the reasons that have led you to do so, and with which relevance? (The scale ranges from1 to 5: 1 = not relevant; 2 = little relevant; 3 = quite relevant; 4 = very relevant; 5 = extremely relevant)

	1	2	3	4	5
Regulatory requirements					
Improvement of strategic planning					
Definition of risk appetite					
Improvement of rating					
Improvement of pricing					
Definition of risk limits/capital allocation					
Assessment of risk-adjusted performance					
Other (specify)					

4.6 At what level are economic capital measures used?

At the global level to assess/allocate economic capital ☐

At business unit level for the evaluation of the risk-adjusted performance ☐

For the evaluation of the profit margin for each product/service ☐

For the evaluation of the profit margin at customer level ☐

Other (specify)_____

4.7 Do you have in place indicators that correlate banking performance to the level of risk?

No ☐

Yes, RAROC (Risk-Adjusted Return on Capital) ☐

Yes, RORAC (Return on Risk-Adjusted Capital) ☐

Yes, RARORAC (Risk-Adjusted Return on Risk-Adjusted Capital) ☐

Yes, EVA (Economic Value Added) ☐

Yes, EaR (Earning at Risk) ☐

Other (specify)_____

4.8 If you do use one or more of the indicators mentioned in the previous question, what are the objectives you want to achieve through their use?

Efficient capital allocation ☐

Assessment of the results achieved compared to the results planned ☐

Comparison of performance between the different business units ☐

Establishment of a system of incentives linked to risk ☐

Other (specify)_____

Comments/details on section 4:

_____

5. Insurance coverage

5.1 Has a comparison been made between insurance contracts and events causing an OR loss?

Yes ☐

No ☐

5.2 If so, has this encouraged a revision (change/renegotiation) of insurance contracts?

Yes ☐

No ☐

5.3 Which organizational areas are involved in management of insurance policies?

OR function ☐

Purchase and logistics ☐

Legal ☐

Other (specify)_____

5.4 Are the traditional insurance contracts supported by more innovating forms of coverage?

Yes ☐

No ☐

5.5 If so, which ones?

_____
_____
_____
_____

Comments/ details on section 5:

_____

6. Trade associations and outsourcing

6.1 Is OR management within the bank supported by tasks performed by trade associations?

Yes ☐

No ☐

6.2 If so, check the tasks performed by the associations

	Regional federation	Italian federation
Supporting in loss data collection		
Supporting in definition of key risk indicators for OR		
Supporting implementation of standardized approach and/or advanced measurement approach		
Advising on insurance coverage		
Supporting in the elaboration of economic capital models		
Disseminating information on OR under the Third Pillar		
Other (specify)		

6.3 Are there any networks among BCCs that support individual banks in OR management?

Yes ☐

No ☐

6.4 If so, who promoted them? _____

6.5 If there is one, which tasks does the network perform on behalf of your bank?

_____
_____
_____
_____
_____

6.6 Have you outsourced any phases of OR management?

Yes ☐

No ☐

6.7 If so, to whom? _____

6.8 In case of outsourcing, which phases are outsourced? _____

Comments/details on section 6:

_____

Please, indicate the regional federation which your bank refers to_____

References

BCBS (Basel Committee on Banking Supervision). 2006. Results of the fifth quantitative impact study (QIS 5), 16 June.

Birindelli, G., and P. Ferretti. 2009. La gestione del RO nelle BCC. In *Il Rischio operativo nelle banche italiane. Modelli, gestione e disclosure*, ed. G. Birindelli, and P. Ferretti. Roma: Bancaria Editrice.

8

Disclosure on OR: Evidence from a Sample of Italian Banks

8.1 Introduction

The current regulatory framework requires banks to provide accurate and comprehensive disclosure of their operational risk profile. In particular, banks are required to disclose the approaches for the assessment of their own funds requirements; they are required to describe the AMA methodology (if adopted), including a discussion of relevant internal and external factors considered in the measurement approach, or (in the case of partial use) the scope and coverage of the different methodologies used.

In order to illustrate the degree of disclosure of the OR management, this chapter reports the results of a survey on a sample of listed banks in Italy, focusing on the following areas of investigation: general aspects; organizational structure; measurement systems; control, mitigation and transfer systems; capital.

G. Birindelli and P. Ferretti, *Operational Risk Management in Banks*,
Palgrave Macmillan Studies in Banking and Financial Institutions,
DOI 10.1057/978-1-137-59452-5_8

8.2 Regulatory Disclosure Requirements

Pillar 3 of the capital adequacy framework requires that banks provide accurate and comprehensive information on their risk profile. In particular, they must disclose their risk management objectives and policies for each category of risk (Article 435—CRR 575/2013), as well as information about their own funds (Article 437—CRR 575/2013). As to market discipline, it is worth remembering that, in the light of the numerous shortcomings of the previous framework evidenced during the international financial crisis, BCBS has been suggesting since 2014 to modify the contents of Pillar 3 (BCBS 2014, 2015, 2016). Overall, the revisions intend to enable market participants to better compare the risk-weighted asset disclosures of the bank, and are focused on improving transparency of the internal model-based approaches adopted for the calculation of the minimum regulatory capital ratios.

According to current provisions, the disclosure requirements are expressed in a document (commonly referred as to Pillar 3 Disclosure, or similar) published by the bank and made accessible through a link on its website. Banks provide information at a level of detail that reflects the organizational complexity and business type. Such information must be arranged on the same basis and abiding by the same criteria used for drafting the financial statement and must be checked by the persons responsible for carrying out the statutory audit of accounts.

With reference to the OR, banks are required to disclose the approaches for the assessment of their own funds requirements; they are required to describe the AMA methodology (if adopted), including a discussion of relevant internal and external factors considered in the measurement approach, and (in the case of partial use) the scope and coverage of the different methodologies used (Article 446—CRR 575/2013).

8.3 Evidence from Italian Banks

In order to illustrate the degree of disclosure of the OR management, we shall review the results from an analysis conducted on a sample of listed banks in Italy; the aim was to check the banks' degree of consistency in reporting and the level of compliance to the disclosure requirements (Birindelli, Ferretti 2009). The information, which was retrieved through both Pillar 3 Reports and Annual Reports, addressed the following areas of investigation:

- general aspects
- organizational structure
- measurement systems
- control, mitigation and transfer systems
- capital.

8.3.1 General Aspects

Among the *general aspects*, we included the definition of OR, the description of the main sources of manifestation of the operational risk, and the illustration of legal disputes.

As to the OR definitions reported, differences were found between Pillar 3 Reports and Annual Reports, with particular regard to the inclusion of legal risk and to the exclusion of strategic and reputational risks (specific details on inclusions and exclusions were missing from the Pillar 3 Reports but were instead reported in the Annual Reports, whereas other times the same information was provided by Pillar 3 Reports and not by the Annual Reports). Nevertheless, the definition of OR resulted to be compliant with the regulatory provisions, with some banks providing a more summary description (in one case only citing the OR sources: internal and external criminal acts, business practices, etc.), while others offering greater detail, for example, by referring to an OR thereby also to the possibility of yielding a lower revenue. Finally, some banks also included compliance risk as part of OR.

Over half of the intermediaries did not dwell on explaining the main sources of manifestation of OR. The remaining provided this information in the Annual Reports, among the quantitative data, except for one bank that recalled the information also in the Pillar 3 Reports. The methods followed to evidence the dynamics of the risk events and their impact are quite heterogeneous, as we observed by the extensive use of tables and pie charts, which were merely descriptive forms. Even the representation of the contents varied: it ranged from the percentage composition of OR sources by event types (in terms of size and impact), to the amount of losses by OR type, with a distinction in gross and net losses, in recoveries and insurance refunds. Often such analysis was completed by the generic indication of improvement interventions on processes and controls with the goal of OR mitigation and of containment of the corresponding losses.

In principle, the situation above also applied to legal disputes. It is worth noting that all banks reported the financial statement items relative to legal controversies under the "Provisions for risks and charges" and that more than half of the sample further detailed the matter within their Annual Reports.

Again the information was heterogeneous: some banks treated the principal legal actions (whether in progress or completed) briefly, while others described in detail the most complex legal disputes (in one case those having petitum exceeding a specific threshold), providing both qualitative (subject and history of the dispute) and quantitative details.

8.3.2 Organizational Structure

The disclosure on OR organizational model was completely disregarded in some cases, since several banks made reference to what has been defined at group level. When present, the description was complete or, in several cases, it involved only few profiles. This was the case of an intermediary who refered only on the main OR control functions: internal audit and compliance. Another intermediary focused only on the reporting activities that were addressed to top management and that dealt with results of the LDC process. Other banks, instead, provided

some details in the Annual Reports: one bank reported on the presence of a centralized function which was dedicated to OR monitoring and collaborated with the officer in charge of the accounts and with internal audit; another institution reported on the activities conducted by the inspection unit, such as development of risk indicators, implementation of information technology support and definition of report contents.

Turning to the institutions that described the organizational structure for OR management in more detail, the first element to be represented was generally the OR framework, where the objectives of the ORM process and the formal assignment of tasks and responsibilities of the bodies involved were also described. In some banks, governance was also mentioned, with the indication of the top management involved in the activities of supervision, management and control.

However, the major focus was attributed to the various functions responsible for the OR management (and in a few cases to the relations among the functions), which mostly overlapped with the description of a head department flanked by peripheral referents. In most cases the head department had responsibilities at group level and was identified with the head OR function or, alternatively, with the OR sector, the risk management direction, the organization, the market and operational risk service. In other cases, reference was made to a general OR management on behalf of the parent company and to many actors involved in their respective areas of competence, such as organization, internal audit, compliance, legal office and supervisory board.

The most common tasks assigned to the head department were the following:

- supervising the methodological and organizational framework;
- defining the methodologies of OR measurement;
- determining regulatory and economic capital;
- checking the effectiveness of mitigation actions;
- supporting the peripheral functions and monitoring the respect of common standards;
- coordinating with other company functions (internal audit, compliance, legal, organization, information technology, etc.);
- reporting in favour of the top management.

The decentralized structures (peripheral referents)—responsible for data collection and control at local level—in some cases resulted to be particularly complex. For example, four officers were identified in one bank: the OR referent (responded to the framework for its own entity); the local OR service (supported the previous one in the realization of the ORM process); the risk champion (supervised the management process for the purpose of validation, in relation to its business, and participated in OR monitoring and defining mitigation measures). Finally, the risk owner (signaled past and/or potential risk events and performed the corrective actions decided). In another bank there was a distinction between referents of the operating and support units and referents of the support units for specific OR types.

Some banks set up a specific OR committee within the parent company. Sometimes, in addition to indicating the committee composition, the bank specified its tasks, such as the periodic verification of OR exposure at group level, the proposal of corrective actions, the suggestion of insurance strategies, the monitoring of the mitigation activities, the examination of the OR reports.

Some banks drew attention towards the monitoring activities of the OR management system performed by the internal audit, also recalling the check conducted on the self-assessment process. As regards the latter, some intermediaries mentioned the definition of the corresponding policy, others specified the responsibilities (again reporting to the area of risk management), and another intermediary dealt with the issue in more detail. Specifically, it reported the establishment of an internal validation process at the parent company and the relevant entities, with the assignment of responsibilities to the decentralized OR functions, who were required to provide a summary on the activities performed and the functions involved and to verify the compliance of the OR management system to both regulatory requirements and group standards. Finally, whenever there was evidence of an area to improve, there was also a description of corrective actions and the timeline for their implementation, when possible.

In less than half of cases the description of the organizational structure was completed by the reminder on the reporting activity underlining the main contents and the recipients. The report was prepared by

the functions responsible for the OR management system and generally addressed: the findings of the qualitative and quantitative modules of the OR measurement; the recoveries; the assessment of the operational losses of greater severity, with identification of the causes; the VaR calculated for the different regulatory event types; the trend of the most significant risk indicators; the measures of prevention and mitigation with indication of effectiveness; the capital absorption. With regard to the periodicity of reporting, only few banks indicated frequency (1 and 3 months), which varied according to the type of information flow produced. The recipients included the top management, the risk committee (and the OR committee if present) and internal audit.

Finally, some intermediaries evidenced the preparation of human resources training programmes, seen as fundamental also because of the cross-cutting nature of the ORs. In order to facilitate the dissemination of the OR culture, one bank declared that it would have addressed the training activities to the top management and operational functions. Another bank mentioned a structured training programme, addressed to all the staff actively involved in the management and mitigation of the ORs. Another bank included training among the tasks assigned to the OR decentralized functions; the head OR function was responsible for informing the peripheral structures about the main regulatory and managerial updates on OR.

8.3.3 Measurement Systems

The interest in the *measuring systems* lies in the willingness to understand the state of progress of the management system and the quantification of the OR by the various intermediaries. The analysis is not only in view of regulatory compliance, but also, and above all, in that of implementation and progressive refinement of the ORM procedures and mechanisms. This is in order to strengthen and valorize decision-making and daily management, keeping with the principle of the use test. These considerations apply not only to the banks adopting AMA, but also to those that, despite using standardized methods, intend to increase their awareness of OR exposure. Just as important for these is

the development of a framework for the identification, collection and classification of the loss data, and also for the assessment of the OR by experts, in order to identify the business areas of greater vulnerability.

Aside from the few banks that did not provide any indication on the measurement systems adopted, and another few that slavishly made reference to the decisions taken at group level, banks provided a description that confirmed the general trend to create (independently of the approach used to calculate capital requirement) loss data collection and self-assessment processes as the main parts of the quantitative and qualitative analysis of the OR. However, among these banks there were significant differences with regard to the developmental stage covered and, consequently, to the related level of detail of the measurement system and of its components. For example, one bank claimed it had been experiencing the process' implementation phase, while another bank stated it had not completed the planning of the LDC, since it considered the development of the risk assessment process as a priority.

All institutions claimed to belong to the Italian Database for Operational Losses, DIPO; one was also part of the Operational Riskdata eXchange Association, ORX, and another also relied on public databases. The reasons for the banks taking part in DIPO were the effective capture of the impacts of extreme events; the integration with internal data; the use as benchmarking tool; the use as reference for the definition of census criteria and data classification; the resolution of interpretation doubts.

Closely linked to the international crisis was the mention by a bank of the activation (within DIPO) of a qualitative flow, which described (without breaching the principle of anonymity) the most significant events reported by the DIPO members in view of creating scenarios concerning specific risk exposures.

Only a few banks delved into the contents of LDC, whose functioning was always accompanied by a supporting IT device. When specified, the census concerned the operational loss data (one bank also mentioned potential losses), the recoveries (not only of the insurance type), the BL of OR manifestation, and further information on the event; collection thresholds were reported only in a few cases. One institution

also reported the periodic riconciliation of the losses with accounting and their real-time updating by decentralized departments.

As to the qualitative module, a generic reference to risk self-assessment prevailed, identified with the procedure (often on an annual basis) of recording and assessing OR exposure and of checking on the adequacy of the controls and of the mitigation measures that have been implemented. RSA was normally conducted by the process owner and was designed to highlight the most vulnerable areas of the bank.

The explicit distinction between scenario analysis and Business Environment and Internal Control Factors (BEICFs) seldom appeared. One bank in particular stated that the analysis of BEICFs—carried out through annual self-assessment on OR control—had a forward-looking value in highlighting the weaknesses of day by day operation. On the other hand, the scenario analysis—this, too, conducted every twelve months and addressed to top management—was designed to measure OR exposure to the single critical issues, in order to understand the changes occurred in the organizational and business context. The financial statements of another bank reported the establishment of a self-assessment process. This process, carried out by the decentralized OR functions, aimed to evaluate the OR exposure at the level of organizational unit and business process, and strengthen the reporting in favour of the other control structures and compliance. The assessment of the operating context coincided with the qualitative analysis of the current ORs exposure that was performed through the assessment of factors of risk in terms of relevance and supervision and aiming to identify areas of vulnerability and possible mitigation actions—in line with a logic of proactive risk management. As emphasized by the bank, the process of self-assessment highlighted the existence of a good OR control and had contributed to the dissemination of a business culture aimed at continuous monitoring of such risks.

The description of the quantitative and qualitative modules had not always been completed with information on the integration process of the components of each module (on the one hand, internal and external data; on the other hand, scenario analyses and BEICFs), and of the modules themselves. Detail on this aspect was only provided by the banks that had already adopted AMA, by those that intended to use it

shortly, inevitably related to the determination of capital requirement for operational risk.

8.3.4 Control, Mitigation and Transfer Systems

With regard to *control, mitigation and transfer systems*, almost all the banks provided information on the business continuity management projects, namely on emergency and business continuity plans, aimed at ensuring the ongoing performance of the activity and at limiting the operational losses in case of serious operational interruptions.

Some heterogeneity was found with regard to other measures of control and reduction of the ORs. Reference was sometimes quite generic. One bank summarized the phases of the mitigation process (analysis of the critical issues and of the solutions in cost/benefit terms; choice, planning and start of the actions, with control on their effectiveness; management of the transfer solutions). Other banks described the variety of the interventions adopted or still to be adopted, including business process re-engineering, outsourcing, corrective actions for the repositioning of the OR at acceptable levels, risk mapping review and recourse to insurance.

Further details were found in other cases. For example, one bank claimed that it had taken steps to regulate the start of businesses in innovative sectors, subjecting start-up to authorization by the board of directors, after having assessed the risks, identified the competent organizational structures, and prepared the control procedures. Another intermediary informed on the functioning of a process addressed to ongoing evaluation of controls for the prevention of fraud risks.

The insurance mechanism for OR transfer was analysed in few cases and in an inconsistent manner: some banks focused on the types of operational risk covered, others on the use of the policies and others, again, on the organizational aspects.

Among the type of insurance contracts, banks mentioned a few specific cases: policies against general risks, and for staff safety; policies safeguarding employees, assets of greater value and cash management; policies including the protection of physical assets, and against the

risk of fraud and on liability. Finally, other policies provided coverage against risks deriving from facts concerning third parties and any damage caused to third parties and thus had appropriate contractual clauses included in the contract as safeguard against damage caused by infrastructure and service providers.

Regarding the use of insurance instruments, one intermediary underlined their adoption in function of reducing unexpected losses; another bank specified that such tools were not employed for supervisory purposes. Finally, a bank declared it had renewed the expiring contracts with the aim of using them to reduce absorption of regulatory capital, once it had fulfilled regulatory standards.

Only one institution underlined the involvement of the OR function in the decisional process related to insurance that consisted in an analysis of OR exposure, of the effectiveness of deductibles, and of limits of the policies. The geographical complexity of this bank had emphasized the need to reduce the differences among the various settings. To this purpose, some policies were grouped at sub-holding level on the basis of the single country, or at group level. In line with the general trend to contract with higher indemnity limits than with lower deductibles, this however was adjusted in consideration of the local interpretation of the companies.

8.3.5 Capital

The last section, *capital*, focuses on the aspect of capital measurement (seen from the perspective of compliance with Pillar 1) and on the quantification of OR exposure for internal purposes. With regard to the first aspect, within the disclosure on capital adequacy, all banks indicated the amount of OR capital requirement, as for the other Pillar 1 risks.

In the case of combined use of the standardized approach and the basic indicator approach, the banks specified the criteria of allocation of the relevant indicators to BLs. One bank described the stages of classification of the activities into the BLs, by distinguishing the mapping of data and the calculation of capital requirement. It first had performed

data mapping at individual level by allocating each management centre in the pertinent regulatory BL; then, it identified the sources of the income figures of these centres and the distribution criteria (in the presence of multiple activities). On the basis of the mapping, each company defined the values according to the management centre, performed the allocation into the BLs, and determined the capital requirement. The same bank finally added that in the case of entities adopting the BIA, it identified the details of the gross income, with particular attention to the intra-group component subdivided by company. For the other intermediaries the allocation of the gross income into the BLs was based on accounting and management principles: one intermediary specified that it used the findings of the ledger that inform the financial statement as well as the data of the management control system.

The issue of economic capital measurement was addressed by only a few banks, sometimes with weak reference to matters concerning the Second Pillar, and never discussed explicitly with regard to OR, but rather, mentioning it in reference to the whole set of banking risks. One intermediary expressed the intention to further explore advanced metrics, in order to estimate the internal capital. Another intermediary specified that the criteria and logics for the calculation of capital requirement were used, in respect of the guidelines defined in the budgeting and planning process, also for the quantification of prospective capital. Two intermediaries claimed that they measured both the economic and regulatory capital to determine capital absorbance per BU through the SA; of these banks one also used an internal model—subject of validation—of the LDA type (see Chap. 6), integrating the information sources related to internal and external data and the RSA scenarios using the Bayesian method. Another bank mentioned the use of ORVaR, based on the Poisson function for the distribution of frequency and on the Weibull or lognormal function for the distribution of severity, in order to asses OR exposure for internal purposes; the forecast of an OR tolerance model moved in the same direction.

The banks that applied AMA or that had applied for authorization to do so dealt with the economic capital when they analysed the method of calculating capital requirement with a good degree of detail.

In a case of prevalidation, the bank carried out an actuarial analysis of internal and external data with a separate study of the frequency and severity of the events and subsequent creation of annual loss distribution by the Monte Carlo approach. The qualitative assessments, processed by means of statistical-actuarial techniques, led to an estimate of unexpected loss, which integrated the former estimate. The capital at risk was defined as the minimum capital—at the consolidated level and net of insurance—as required in order to cope with maximum potential loss. Such capital was estimated through LDA, applied to the quantitative data and to the results of the scenario analyses over a one-year time horizon and with a confidence interval equal to 99.96%. The effectiveness of internal controls set up in the operating units was assessed by applying a correction factor resulting from the risk analysis of the operating context.

As for the intermediaries already authorized to use AMA, one bank confirmed that for the purpose of risk capital calculation the classes it had taken into account corresponded to the types of operational event. All classes were estimated separately for frequency (only on internal data) and severity (on internal and external data and on scenario analysis), in order to reach a distribution of annual losses through simulation, taking into account insurance coverage. Each class was adjusted in function of risk indicators; stochastic dependence among the various risk classes was obtained on the basis of internal data; the annual loss distributions, realized for each class, were aggregated through copula functions using the t-Student method. The capital at risk was calculated in relation to aggregate loss distribution at a confidence level of 99.9%, as required by the supervisory regulations, and of 99.97% for the determination of the economic capital. Allocation mechanisms allowed identifying capital absorption of each entity reflecting the efficacy of the OR management process.

Also another bank authorized to use AMA had adopted a mixed model LDA-Scenario type. The quantitative component was based on the collection, analysis and statistical modelling of the internal and external data; capital calculation took into account the seven categories of regulatory events through Extreme Value Theory (EVT) techniques (Chap. 6); the frequency and severity were estimated according to event

types. The qualitative component was focused on the evaluation of the units' risk profile and on the identification of relevant scenarios; statistical techniques attributable to the credibility theory were used for its integration. The output of the measurement model, obtained at group level, was reallocated on the basis of historical loss criteria, of top management estimates and of income information (such as gross income) and used for internal purposes.

Some of the considerations reported by this latter bank were particularly interesting, especially in reference to the positive implications of the use of AMA, which had allowed a more conscious OR management, ensuring a progressive reduction of the related exposure. The need was emphasized to closely monitor the initiatives of integration and corporate reorganization that had been undertaken, since they were strongly insidious in terms of OR exposure. The concern that the changes induced by similar processes might have constituted a dangerous source of operational risk exposure was also evidenced from the reading of the financial statement, which evidenced that suitable scenario analyses had been conducted to assess the risks associated with disfunctions or inadequacies in the processes, in information systems or in the management of human resources, with specific reference to merger and acquisition operations.

8.4 Conclusions

Overall, the reports clearly evidence a heterogeneity among information provided. In particular, the descriptions provided by the participating banks offer little insight on the specific features of the operational risks management, measurement, control and mitigation systems implemented, and prevent an extensive comparison of measures taken by banks to manage their OR exposures. As to the comparability of the results, this too was affected by the low degree of uniformity of the subjects analysed and the uneven level of detail among the various areas of disclosure. Indeed only a few institutions covered all the areas of disclosure with equal accuracy, while the majority provided detailed

information limitedly to very few areas leaving all the other areas scarcely addressed, if not addressed at all.

The different degree of disclosure provided by the banks and the different relevance of the various areas of disclosure, with an emphasis on some aspects compared to others, can be easily verified by assigning a score to each of the items forming each area of disclosure. Based on the information in the previous sections, we have selected the indicators which are most significant in our opinion and which fall into four areas. We have then assigned a rating of disclosure to each bank by means of the sum of partial scores that take into account (in all except one case) the amplitude and deepening of the contents of the information produced[1]. A summary of the indicators, classified by area of disclosure, and the assignment criteria of the relative scores appear in Table 8.1.

Table 8.1 Assignment of the disclosure rating (own processing)

Areas of disclosure	Indicator	Score
General aspects	OR definition Main sources of OR Legal disputes and possible losses	For all the indicator (unless otherwise said), the score is: 0 = information is missing 0.5 = information is not clear or comprehensive 1 = information is clear and comprehensive
Organizational structure	Preparation of the OR framework Formalization of the governance mechanism Organizational functions involved and their tasks Inter-relations among the organizational functions Internal validation Reporting Training	
Measurement systems	Method adopted for calculating the capital requirement for OR Use of mitigation tools for reducing the capital requirement Analysis of the OR measurement for internal purposes Methods for calculating the economic capital for OR	0 = information missing; 1 = information provided
Control and mitigation systems	Mitigation and transfer tools Business continuity management	

The assignment of scores to each item and the relative sum leads to ratings that range from a minimum value of 2 to a maximum of 14, with wide dispersion with respect to average, equal to 5.9. High variability of information provided by banks can be easily understood by a chart that ranks all the banks with respect to average value (Fig. 8.1).

As expected, the intermediaries with higher rating (equal or superior to 10) are already using AMA, and are flanked by institutions strongly aimed at achieving the most advanced methodology in the short term.

However, the different levels of openness to disclosure of the four areas may be understood by comparing the difference, calculated for each area and compared to the maximum possible score, between the latter and the average score (Table 8.2). Even in this case the deviations are in line with our expectations: the sections most wealthy on information refer to the general aspects and to the control and mitigation systems; whereas the measurement systems and—more importantly—organization are less explored. These latter areas are the most articulated in terms of requirements, although with different types of prevailing information: the area containing more descriptive information (organization) indicates wider refinement and in-depth spaces, pointing out that the transmission of quality contents—which for their very nature may be liable to vague statements—limits the level of disclosure.

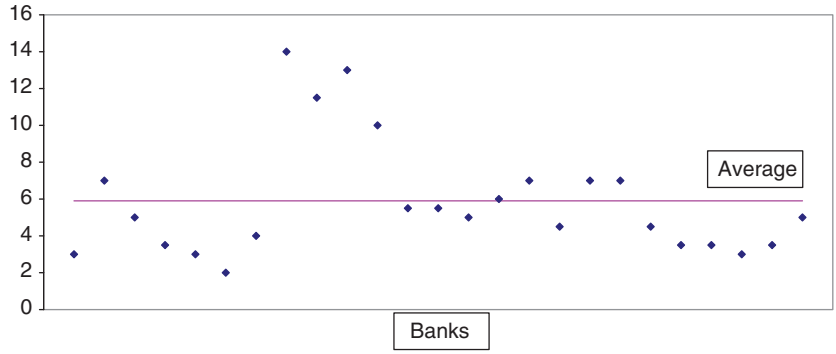


Fig. 8.1 The disclosure rating (own processing)

Table 8.2 Areas of disclosure: average and maximum value (own processing)

Areas of disclosure	Number of indicators	Average score	Maximum score	Maximum score—average score
General aspects	3	1.9	3	1.1
Organization	7	1.7	7	5.3
Measurement systems	4	1.4	4	2.6
Control and mitigation systems	2	0.8	2	1.2

Note

1. Despite our awareness of the discretional nature embedded in grading the information in function of its contents, we preferred follow this approach for all indicators featuring extremely heterogeneous levels of detail. Only in one specific case we opted to assign the score based on the absence/presence of the indicator.

References

BCBS (Basel Committee on Banking Supervision). 2014. Review of the Pillar 3 disclosure requirements, June 2014.

BCBS (Basel Committee on Banking Supervision). 2015. Revised Pillar 3 disclosure requirements, January 2015.

BCBS (Basel Committee on Banking Supervision). 2016. *Pillar 3 disclosure requirements—consolidated and enhanced framework*. Consultative document, March 2016.

Birindelli, G., and P. Ferretti. 2009. *Il rischio operativo nelle banche italiane*. Roma: Bancaria Editrice.

Index

A

Advanced Measurement Approach (AMA) 15, 24, 37, 38, 47, 170, 177
Alternative Risk Transfer (ART) 124

B

Bank 2, 4, 5, 12, 13, 22, 26, 29, 32, 33, 43–50, 58, 62, 69, 70, 72, 76, 83, 90, 97, 100, 103–105, 112, 116, 117, 119, 120, 122, 124, 125, 127, 136, 138, 154, 161, 162, 170, 173, 175, 176, 180, 182–184, 200, 202–213
Basel Committee on Banking Supervision (BCBS) 2, 14, 29–32, 32, 37, 38, 63–65, 69, 70–72, 76, 95, 98, 101, 102, 113, 122, 123, 170, 186, 200
Basel II 2, 14, 28, 33, 38, 65
Basel III 2, 3, 38, 65
Basic Indicator Approach (BIA) 37–39, 170, 177
Board of directors 4, 68, 70, 72, 73, 80, 82, 98, 105, 173, 177, 180
Boundary loss 72, 178
Business continuity 82, 84, 89, 102, 105, 208, 213
Business Environment and Internal Control Factors (BEICF) 48, 49, 60, 96, 153, 177–180
Business line (BL) 1, 19, 20, 33, 40–43, 45, 46, 49, 55, 74, 76, 83, 92, 135, 139, 140

C

Calculation dataset 135, 137, 140
Capital adequacy 38, 39, 200, 209

G. Birindelli and P. Ferretti, *Operational Risk Management in Banks*, Palgrave Macmillan Studies in Banking and Financial Institutions,
DOI 10.1057/978-1-137-59452-5

Capital requirement 2, 3, 13, 20, 21, 24, 37, 38, 43, 45–48, 50–53, 62, 64, 79, 111, 113–116, 134–136, 170, 176, 185, 208–210, 213
Capital Requirements Regulation (CRR) 2, 14, 38
Claim 16, 112, 114, 126–130, 185
Compliance
  function 32, 91, 94–96
  risk 9, 21, 28–33, 94–96, 201
Cooperative bank (BCC) 7, 169, 170
Coverage 37, 38, 54, 62, 79, 82, 112–116, 118, 119, 122, 125–131, 159, 169, 182, 200, 209, 211
Credit risk 2, 14, 20–22, 47, 50, 58, 137, 170

D
Database
  set 56
Date
  of accounting 56, 135, 140
  of detection 135, 136
  of discovery 56
  of occurence 56, 95, 135, 136
Disclosure 6, 17, 64, 171, 199–202, 209, 212–215

E
European Banking Authority (EBA) 50–53, 55–59, 73, 93, 112–114
Event type 16, 33, 45, 49, 55, 62, 95, 100, 120, 123, 124, 131, 138, 140, 202, 205
Expected loss 48, 54, 91, 117, 134, 179
External data 48–50, 52, 55, 58, 59, 113, 137, 154, 157, 162, 178, 180, 207, 210, 211
External factors 199, 200
External fraud 17, 123

F
Financial
  collapse 1, 4, 11, 12, 32, 67, 68
  crisis 1, 2, 19, 38, 39, 68, 200, 206
  institution 1, 5, 11, 12, 15, 19, 20, 24, 25, 27, 38, 89, 125, 126, 206
  scandal 1, 13, 27, 32
Framework 2–4, 6, 13, 33, 37, 38, 42, 44, 46, 49, 52–54, 59, 62, 64, 65, 70, 71, 74, 75, 78–81, 83, 87–89, 102, 105, 112, 113, 159, 199, 203, 213
Fraud 12, 15, 20, 21, 23, 28, 58, 103
  external 16, 22, 30, 95, 124, 174
  internal 4, 16, 22, 29, 30, 68, 92, 136
Frequency 16, 19, 55, 61, 90, 91, 99, 117, 118, 137, 141, 155, 157, 160, 177, 178, 180, 205, 211
Frequency distribution 134, 146, 157

G
Governance 4, 6, 39, 44, 52, 53, 67, 68, 73, 93, 99, 102, 203, 213

I
Information technology 20, 27, 69, 81, 99, 125
Insurance 4, 6, 50, 52, 54, 55, 80, 111–113
  coverage 7, 77, 80, 89, 112, 114, 118, 120, 122, 130, 160, 171
  policies 4, 62, 77, 82, 103, 113–116, 118, 120, 182
Insurance mapping process 113
Insurer 55, 112, 114, 115
Internal audit 6, 20, 46, 47, 68, 71, 72, 81, 84, 91–93, 103, 104, 160, 172, 173, 176
Internal Capital Adequacy Assessment Process (ICAAP) 39, 172
Internal data 48, 49, 52, 54–59, 113, 122, 137, 162, 178, 180, 206, 211
Internal factors 199, 200
Internal fraud 17, 123
Internal process 2, 14, 29, 31, 137
Italian banks 7, 201
Italian Database for Operational Losses (DIPO) 30, 137, 206

K
Key risk indicator (KRI) 47, 72, 90, 98, 160, 177

L
Legal risk 2, 14, 15, 25, 28–32, 56, 62, 174, 176, 201
Loss 2, 4, 10, 11, 13, 14, 16, 21, 22, 24, 26
  data 3, 21, 43, 56, 60, 82, 95, 96, 138, 141, 143, 151, 161, 162, 164, 177, 206
  event type 16
Loss Data Collection (LDC) 46, 75, 82, 95, 104, 173, 183, 186
Loss Distribution Approach (LDA) 5, 133, 134

M
Market risk 2, 10, 14, 20, 21, 23, 24, 32, 42, 53, 57, 135, 179

O
Operational loss 2, 4, 16, 17, 39, 45, 64, 79, 93, 96, 98, 120, 131, 135, 136, 144, 208
Operational risk (OR) 1, 2, 4–7, 9, 10, 13, 14, 19–23, 25, 28–30, 32, 33, 37, 38, 43, 44, 52, 65, 67, 70, 71, 74, 76–82, 84, 87, 88, 91, 92, 95, 97–100, 103, 104, 106, 116, 117, 130, 134, 135, 145, 148, 150, 151, 159, 163, 170, 180, 184, 201, 208
Operational risk Committee (OR) Committee 76, 77, 80, 82, 84, 87, 97
Operational risk (OR)culture 70, 73, 173
Operational risk event (OR) event 95, 156
Operational risk function (OR) function 32, 72, 85, 87, 173, 176

Operational risk management (ORM) 2–7, 9, 14, 19, 25, 39, 52, 54, 65, 67, 70, 72, 74, 75, 83, 87, 93, 105, 106, 130, 131, 169, 173, 176, 212, 213
Operational risk mitigation techniques 111
Operational risk modelling 6, 133
Organizational structure 7, 42, 67, 68, 75, 92, 163, 184, 185, 199, 201, 204, 208
Outsourcing 18, 118, 169, 171, 184, 208
Own fund requirement 6, 22, 25, 39, 40, 43, 51, 53, 55, 56, 60, 61, 65, 116, 199, 200

P
Pillar 3 6, 38, 64, 200–202

Q
Qualitative standard 47, 52, 64
Quantitative standard 47, 48, 52, 54

R
Recovery 22, 55, 103, 112, 122–124
Regulatory framework 3, 6, 64, 112
Regulatory Technical Standards (RTS) 50–52
Relevant indicator 39, 40, 42–46, 88, 209
Reporting 6, 11, 21, 43, 58, 72, 75, 80, 83, 95, 97, 98, 172, 174, 175, 177, 201, 204, 205, 207
Reputational risk 2, 14, 21, 26, 27, 31, 127, 176, 201
Risk self assessment 88, 95
Risk transfer mechanisms 50, 52–54, 111, 112, 115

S
Scenario analysis 48, 52, 55, 72, 92, 135, 157, 161, 163, 178, 180, 207, 211
Scenario Based Approach (SBA) 6
Scope of operational risk 15, 24–26
Second Pillar 7, 169, 171, 180, 210
Senior management 4, 42, 43, 68, 70–74, 94, 97–99, 105
Severity 19, 55, 59, 61, 91, 99, 117, 137, 141, 142, 144, 152, 156, 157, 160, 178, 205, 210, 211
Severity distribution 134, 142, 157
Standardised Approach (SA) 38, 39, 42–47, 76, 121
Standardised Measurement Approach (SMA) 64
Strategic risk 15, 21, 25, 26, 176
Supervisory authority 3, 46
Survey 7, 59, 153, 169–171, 175, 182, 184, 199
System 2, 4, 7, 11, 14, 15, 17–19, 23, 26, 27, 29–32, 42–49, 51–54, 60, 61, 67–71, 74, 75, 78, 87, 89, 92, 93, 95, 98, 99, 106, 113, 117, 118, 123, 126, 129, 152, 169, 171, 173, 174, 176, 177, 185, 186, 199, 201, 205, 206, 210, 212–215

System failure 16, 100

T
Top management 67, 118, 127, 172–174, 202, 205, 207, 212

U
Use test 47, 52, 63, 92, 205

V
Value at Risk (VaR) 62, 134, 146, 152