

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.

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	<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • Theft and fraud (theft, robbery, forgery, check kiting) • Systems security (hacking damage, theft of information without monetary loss)
Employment practices and workplace safety	<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • Disasters and other events (natural disaster losses; human losses from external sources—terrorism, vandalism)
Business disruption and system failures	<ul style="list-style-type: none"> • Hardware; software • Telecommunications; utility outage/disruptions

(continued)

Table 2.1 (continued)

Execution, delivery and process management	<ul style="list-style-type: none"> • 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 sub-prime 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.



<http://www.springer.com/978-1-137-59451-8>

Operational Risk Management in Banks
Regulatory, Organizational and Strategic Issues

Birindelli, G.; Ferretti, P.

2017, XII, 221 p. 5 illus., Hardcover

ISBN: 978-1-137-59451-8

A product of Palgrave Macmillan UK