

2

Operational Risk Management: Regulatory Framework and Operational Impact

Paola Leone and Pasqualina Porretta

Abstract Banks must establish an independent Operational Risk Management function aimed at defining policies, procedures and methodologies for identifying, measuring, monitoring and controlling operational risks. In this perspective, this chapter analyses (a) the regulatory framework on the operational capital requirement; (b) the regulatory view on Operational Risk Management; and (c) the new Supervisory Review and Evaluation Process (SREP) in relation to operational risk. The chapter also attempts to propose an integrated approach able to defining, managing, monitoring and reporting operational losses together with capital planning, ICAAP (*Internal Capital Adequacy Assessment*

Although this chapter has been prepared by both authors jointly, § 2.2, 2.4, 2.8, 2.10, was written by Paola Leone, whereas §§ 2.1, 2.3, 2.5, 2.6, 2.7, 2.9 by Pasqualina Porretta.

P. Leone · P. Porretta (✉)
Sapienza University of Rome, Rome, Italy
e-mail: pasqualina.porretta@uniroma1.it

P. Leone
e-mail: paola.leone@uniroma1.it

Process), RAF (*Risk Appetite Framework*) and risk culture of financial intermediaries also in accordance with the new SREP perspective.

Keywords Operational regulatory framework • Operational risk management • Operational Risk Supervision • New SREP

2.1 Operational Risk Management in the Banking System: First Considerations

As mentioned in the previous chapter, operational risk differs from other banking risks because normally it is not incurred directly in view of a profit, but it is inherent the actual implementation of the institution's activity, thus affecting its management modalities. However, an operational risk inadequately managed can translate into a distorted image of the institution's risk profile and expose it to heavy losses. Given the particular nature of operational risk, Operational Risk Management—that is the identification, assessment, monitoring and control/mitigation of the mentioned risk—assumes particular relevance for financial intermediaries with greater operational complexity. However, this function is still in embryonic phase, waiting for an adequate organizational and strategic collocation. For several years now, Authorities have been emphasizing its relevance by issuing an enormous amount of guidelines and sound practices.

Over the years, banks have used various tools to identify and assess operational risks, among which:

- *Self-assessment*, that is the bank's analysis of its operations and activities against a range of potential vulnerabilities to operational risk. This method is endogenous and often makes use of control lists and/or work groups to identify the points of strength and weakness of the institution's context of operational risk. Scorecards, for instance, constitute a tool for translating qualitative assessments into quantitative parameters on the basis of which a score is given to the different types of exposure to operational risk. Some scorecards refer to peculiar risks

typical of a specific operational area, while others refer to risks that fall transversally within various fields. These scorecards may consider not only risk factors, but also related mitigation techniques. They can be used to allocate economic capital to the various business lines on the basis of the results obtained by managing and controlling the various aspects of operational risks;

- *Risk Mapping*, that is the classification of operational units, organizational functions and process flows on the basis of the different type of risk. The exercise can identify possible critical areas and thus foster the definition of priorities for subsequent management interventions;
- *Risk indicators*, that is statistic and/or numeric quantities, often of financial nature, capable of providing useful elements for knowing a bank's operational risk position. They are generally subject to a periodical review (for instance, every month or every three months) with the aim to call the bank's attention towards the possible onset of critical areas. Examples of risk indicators are the amount of failed transactions, the personnel's rotation rates, the frequency and/or seriousness of errors and omissions; and
- *Measurement of operational risk exposure through various approaches*. For instance, historical data losses incurred by the bank can provide useful information for assessing exposure and defining control/mitigation policies. For said data to be validly used, it is necessary to develop a methodological framework able to identify systematically the frequency, seriousness and other relevant aspects of the single events that generate loss. Moreover, some banks integrate internal losses with external ones as well as with scenario analyses and risk assessment factors.

In order to manage operational risk adequately, *an effective monitoring process* needs to be carried out. Regular monitoring fosters a quick identification and correction of possible lacks related to policies, processes and procedures in Operational Risk Management. In turn, this can considerably reduce the potential frequency and/or seriousness of loss events.

Besides monitoring loss events, banks should define indicators capable of identifying in advance risk increases of future losses. Therefore,

said indicators (often defined '*key risk indicators*' or '*early warning indicators*') need to be forward-looking and may consider as potential sources of operational risk factors the quick business expansion, the introduction of new products, the personnel's turn over, operational blockings, periods in which systems are still and so on. Since these indicators are directly connected to specific threshold values, the monitoring process can contribute effectively to identify substantial risks in a transparent way, enabling banks to react adequately.

The frequency of the monitoring should depend on the dimension of the risk, as well as on the frequency and nature of operational losses. Monitoring should constitute an integrating part of the bank's activity. The results of this activity should be inserted in a report transmitted to the management and to the Board, together with conformity analyses provided by the functions of internal audit and/or risk management.

Banks should have policies, processes and procedures for controlling and/or mitigating relevant operational risks. In other words, banks should be able to decide:

- in case of controllable risks, whether to use control procedures and other appropriate techniques, that is to undertake the actual risks;
- in case of risks that are not controllable, whether to undertake them, reduce the range of the activity or totally interrupt it.

Besides establishing control processes and procedures, banks should develop a framework capable of assuring compliance with a set of internal policies related to the risk management system, integrated with a sound culture of control, promoting correct behaviours in Operational Risk Management. The Board and the senior management are in charge of fostering said culture, which must become an integrating part of the bank's normal activities.

According to the current regulatory framework, in fact, the Board of Directors are called to:

- approve and implement a system at company level developed expressly to manage operational risk as a distinct typology of risk, for the bank's security and resilience;
- establish a managerial structure capable of implementing the bank's Operational Risk Management;
- review the system periodically to make sure that the bank is managing the operational risks arising from changes in the market and other external factors, or from the introduction of new products, activities and systems; and
- activate a rigorous and organized process of internal audit.

The senior management should translate the principles of the Operational Risk Management system developed by the Board into:

- specific policies, procedures and processes implementable and verifiable within the scope of action of the bank's various business units;
- making sure that:
 - i. the bank's activities are carried out by qualified personnel;
 - ii. the bank's Operational Risk Management policies have been communicated with clarity to the personnel at all levels in the units in which there are relevant operational risks; and
 - iii. the personnel in charge of managing operational risks communicate effectively with the personnel in charge of credit risks, market risks and any other type of risks, as well as with offices in charge of purchasing external services, such as insurance and outsourcing services.

The issue concerning the assessment of operational risk events has already been covered in the previous chapter. The following paragraphs will provide a brief overview of the regulatory methodologies for measuring the operational capital requirement.

2.2 Regulatory Approaches for Measuring Capital Requirements. An Introduction

Basel II introduced for the first time an explicit capital requirement even for operational risks, whose rules and regulations are therefore equated with those of market and credit risks. The prudential treatment of operational risk lies in the estimate of three methodologies for calculating the capital requirement that is the *Basic Indicator Approach*, BIA; the *Traditional Standardized Approach*, TSA; and the *Advanced Measurement Approach*, AMA. These three regulatory approaches for calculating the operational risk capital are characterized by an increasing level of sophistication and risk sensitivity.

2.2.1 Basic Indicator Approach

The Basic Indicator Approach—currently regulated by Articles 315 and 316 of Regulation (EU) No. 575/2013 of 26 June 2013 (Capital Requirements Regulation or CRR, implementing Basel III)—is characterized by its simple calculation and accessibility due to the absence of specific requirements for the banks wanting to use it. However, it reveals scarce correlation with the risk incurred by the single institutions, because the calculation parameters are not defined on the basis of the institution's historical data, but at system level. Under the Basic Indicator Approach, the own funds requirement for operational risk is equal to 15% of the average over three years of the relevant indicator as set out in Article 316. Institutions shall calculate the average over three years of the relevant indicator on the basis of the last three twelve-monthly observations at the end of the financial year. When audited figures are not available, institutions may use business estimates. This indicator (intermediation margin (IM)) is approximable to an amount of the correlation between the total volume of the banking activity, expressed by the exposure indicator, and the operational risk. The correct 'calibration' of the coefficient used to approximate the relationship between the volume of operativeness and the related level of exposure to the operational risk arising from it, results to be a key aspect in this

approach. The three-yearly average is calculated on the basis of the last three positive observations on annual basis carried out at the end of the fiscal year. Therefore, the formula is:

$$K_{BIA} \frac{\sum_{i=1}^3 IM_i \alpha}{3}$$

where:

K_{BIA} = the capital requirement under the Basic Indicator Approach.

IM_i = the intermediation margin related to a given year that is one of the last three years in which the gross income achieved was positive. For institutions applying accounting standards established by Directive 86/635/EEC, based on the accounting categories for the profit and loss account of institutions under Article 27 of CRR, this indicator is the sum of these elements with their positive or negative signs: (1) interest receivable and similar income, (2) interest payable and similar charges, (3) income from shares and other variable/fixed-yield securities, (4) commissions/fees receivable, (5) commissions/fees payable, (6) net profit or net loss on financial operations, (7) other operating income

α = a fixed percentage, set by the Basel Committee (currently 15%).

An aspect worthy of particular attention concerns the choice of the intermediation margin as proxy of the exposure to operational risk. In this regard, there are several perplexities concerning the use of said indicator to express the dimension of banking operativeness and concerning the relationship (fixed percentage established by the Basel Committee) assumed by the regulatory framework between the amount of said indicator and the exposure to operational risk. Operational risks connected to catastrophe events or other external factors do not present any type of relationship with the broadness of the mentioned margin. On the contrary, it has been observed that a larger volume of the intermediation margin allows to mitigate the impact caused by operational losses,

especially those characterized by greater severity. Therefore, on the basis of empirical evidence, there seems to be an inverse relationship between the intermediation margin and the capital requirement with respect to operational risk. Hence, the key characteristics of the Basic Indicator Approach are two: on the one hand, the easy calculation and the effortless data collection, and on the other hand, the inadequacy in considering the different operational riskiness of the various activities carried out by a bank. The simplistic connotation of this approach helps understand the absence of specific recommendations concerning its adoption, in any case, subject to compliance with the general principles of operational risk governance and management. It is also important to highlight that this model tends to adapt better to smaller realities, due to the modest level of operational diversification and the moderate complexity of measurement systems that generally characterize smaller banks.

2.2.2 Standardized Approach—SA

The **Standardized Approach**—regulated by Articles 317 and 318 of the CRR—requires the division of the bank's activities into eight business lines and differs the capital requirement on the basis of the risks related to each business line. The Standardized Approach defines capital requirement as the three-yearly average of the sum of the annual requirements for all business lines, which in turn are calculated by multiplying a factor (denoted beta) by an indicator (intermediation margin in a given fiscal year for a given business line) assigned to the specific 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 with positive own funds requirements in other business lines without limit. However, where the aggregate own funds requirement across all business lines within a given year is negative, institutions shall use the value zero as the input to the numerator for that year. As underline in the Article 318 (CRR), business line mapping must be well documented; institutions shall develop and document specific policies and criteria for mapping the relevant indicator for current business lines and activities into the standardized framework. They shall review and adjust those policies and criteria as appropriate for new or changing business activities and risks.

The ratio of the Standardized Approach implies that banks whose business lines are particularly risky in terms of operational risk must hold a higher capital considering said exposure. The formula for calculating the capital requirement against the operational risk through the Standardized Approach is expressed as follows:

$$K_{SA} \frac{\left[\sum_{k=1}^8 (IM_k \beta_k)_i; o \right]}{3}$$

where:

- K_{SA} = the capital requirement under the Standardized Approach;
- IM_k = the intermediation margin in a given fiscal year for a given business line; and
- β_k = a fixed percentage (set by the Committee) which refers the level of required capital to the level of intermediation margin for each of the eight business lines.

Analogously to what already observed previously with reference to the α coefficient, the β coefficients express a measure of the relationship between the volume of operativeness connected to the different business lines and the correlated risk of losses. The β factor is a proxy of the relationship existing within the entire sector between operational risk losses, historically identified in a specific business line, and the aggregated value of the intermediation margin for the same line.

With reference to each specific business line, the β factor is defined as indicated in Table 2.1.

In order to use the Standardized Approach, institutions must fulfil several criteria provided for by European regulations as mentioned under Article 320 of the CRR. Said criteria—however, less strict than those indicated in the previous version of the regulatory framework (Basel II)—are as follows:

- The bank must be provided with a well-documented Operational Risk Management and assessment system, with clearly appointed responsibilities. Said system, subject to periodical independent

Table 2.1 Business line. *Source* Basel Committee on Banking Supervision

Corporate finance	18% IM
Trading & sales	18% IM
Retail banking	12% IM
Commercial banking	15% IM
Payment & settlement	18% IM
Agency services	15% IM
Asset management	12% IM
Retail brokerage	12% IM

reviews carried out by internal or external auditors, is aimed at identifying exposures and relevant data on operational risk, including significant losses.

- The operational risk assessment system must be closely integrated into the bank's overall risk management process of the institution. Its output shall be an integral part of the process of monitoring and controlling the institution's operational risk profile.
- The bank must implement a communication system with the senior management so as to provide reports to those in charge of the various functions concerning the institution's exposure to operational risk.
- The bank must develop procedures that allow to carry out appropriate actions on the basis of the information provided in said reports.

This methodology is more complex and refined compared to the previous one since, keeping into account the composition of the bank's portfolio activities, it allows to identify several differences in the risk profile. However, the adoption of β coefficients set by Supervisory Authorities (derived from the data system) limits the capability of this approach to represent the bank's real risk profile. The SA approach does not allow to obtain precise information on the causes of operational riskiness, with inevitable prejudice towards the development of adequate Operational Risk Management strategies and techniques.

Moreover, the hypothesis of a perfect correlation among the various loss events is criticizable, under the assumption that the operational losses of the various business lines are identified contextually, thus requiring for the bank to hold a sufficient capital in order to face the

combined events. Lastly, it is important to highlight that the potential capital saving associated with the adoption of the Standardized Approach instead of the BIA—because more adherent to the risk profile of each single bank—strongly depends on the business lines in which the single banks generate a greater volume of intermediation margin. In fact, with reference to the prevailing nature of the activities carried out, it is possible for a bank to generate most of its intermediation margin in the business lines with the highest levels of the β coefficient (18%). In said circumstances, it may be necessary to hold a higher capital for regulatory purposes, compared to when the Basic Indicator Approach is applied, despite the risk profile being the same.

2.2.3 Alternative Standardized Approach—ASA

The national Supervisory Authorities have discretionary powers to allow a bank to use the Alternative Standardized Approach (ASA), as long as the institution is able to prove that by using the Standard Approach some risks would result overestimated and that the ASA can offer a better basis, for instance, to avoid duplications in calculating risks.

In particular, Article 319 (CRR)—based on the same rules set out in the Basel Accord—provides for institutions to apply, for the business lines ‘retail banking’ and ‘commercial banking’, the relevant indicator is a normalized income indicator equal to the nominal amount of loans and advances multiplied by 0.035. To be permitted to use the Alternative Standardized Approach, an institution shall meet all the following conditions:

- a. its retail or commercial banking activities shall account for at least 90% of its income;
- b. a significant proportion of its retail or commercial banking activities shall comprise loans associated with a high PD; and
- c. the Alternative Standardized Approach provides an appropriate basis for calculating its own funds requirement for operational risk.

The underlying motivation for applying an indicator of normalized income is ascribable to the difficulties that banks could incur in disaggregating loans and advance payments related to activities falling within the retail business line from loans and advance payments related to activities falling within the commercial business line.

In order to calculate the capital requirement, beta coefficients remain unvaried for the two mentioned operational lines (respectively, 12% and 15%), and it is possible to aggregate the two lines using a beta equal to 15%. Even this method follows the treatment reserved to negative values of the annual capital requirement described in the Standardized Approach. Therefore, the total capital requirement under the ASA is the simple sum of the coefficients of each of the eight business lines:

$$K_{ASA} = \frac{\left[\sum_{i=1}^2 (IM_i \beta_i) + \sum_{i=3}^4 (LA \beta_i m) + \sum_{i=5}^8 (IM_i \beta_i) \right]}{3}$$

where:

K_{ASA} = the capital requirement under the Alternative Standardized Approach (ASA);

IM_i = the level of the exposure indicator for the given business line (intermediation margin: the average annual income resulting from the three previous fiscal years for each of the six business lines);

β_i = a fixed percentage, set by the Committee, for the given business line;

m = a fixed factor set by the Committee (currently equal to 0.035); and

LA = the average over the last three fiscal years of the total loans and advance payments (not pondered for the risk and net of allocations) of the retail business line and the commercial business lines (that is, business lines 3 and 4).

2.3 Advanced Measurement Approaches (AMA)

The last approach proposed by the Basel Committee for measuring and managing operational risk (AMA) is not identifiable, like the BIA and SA, as an analytical formulation, but it gives the possibility to use a wide range of models, characterized by a growing level of risk sophistication and sensitivity. The Basel Committee's decision to propose a set of models—instead of a single one—for measuring risk is aimed at providing banks with a broad flexibility in processing the methodology used for calculating capital requirement, so as to make it consistent with the bank's business model and related operational risk profiles.

The Supervisory Authority authorizes banks that fulfil specific quantitative and qualitative requirements—besides company governance mechanisms and organizational requirements with reference to internal controls and Operational Risk Management system—to calculate capital requirement for operational risks with analytical measurement models capable of expressing the absorption of economic capital associated with this typology of risk. This permits to represent the riskiness of a bank's activity more appropriately. Therefore, the AMA offer the advantage of a more accurate measurement of the exposure to operational risk, because developed ad hoc for the single bank.

In principle, the AMA entail a reduction of the operational capital requirement for three main reasons:

- They allow to keep into account the correlation effects among the risk level of the various business lines. The Committee recognizes said possibility, as long as correlation estimates are based on a rigorous and sound methodology, capable of reflecting the uncertainty of which they are typically characterized.
- They allow to obtain capital discounts against the use of insurance policies. In other words, banks that adopt the AMA can recognize insurance products as mitigation factor to operational risk exposure in the calculation of the related capital requirement.

- They allow the exclusion of expected losses from the capital value to allocate with respect to operational risk, as long as banks are able to prove to the Supervisory Authority to have kept into account the expected losses in the allocations to risk funds and in product pricing. The Basel Committee does not limit the bank's choice concerning the approach to use in calculating the capital requirement, although it subjects the use to the fulfilment of qualitative and quantitative criteria. In particular, three possible methodologies are proposed under the AMA: the Internal Measurement Approach (IMA), the Scorecard Approach and the Loss Distribution Approach (LDA) (Fig. 2.1).

2.3.1 Internal Measurement Approach

In the Internal Measurement Approach, the capital requirement is calculated assuming a stable relationship (linear, but even more complex) between unexpected losses and expected losses. Operational expected losses are defined similarly to credit risk that is combining estimates of probability of loss event (PE) with the impact that it can produce (LGE), on the basis of historical data, with an exposure indicator (EI), making

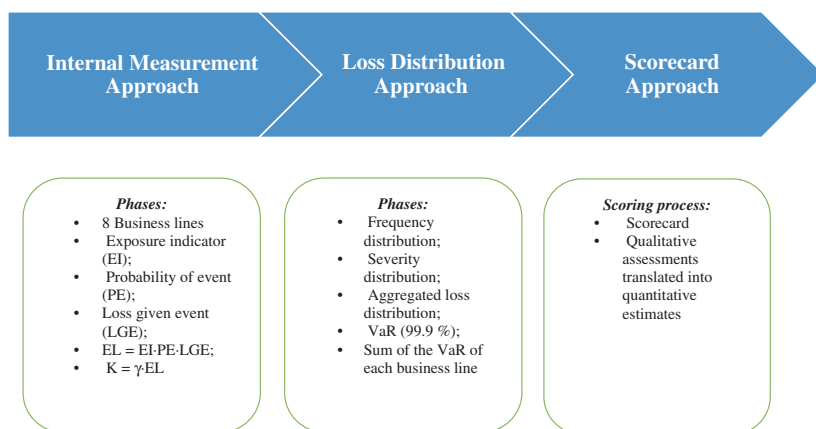


Fig. 2.1 AMA methodologies. *Source* Authors' elaboration

a distinction for each business line and each event type. Basically, assuming a linear relationship, with coefficient γ , between absorption (K) and expected losses (EL), for event i of business line j , the formula is:

$$K_{i,j} = \gamma_{i,j} * EL_{i,j} = \gamma_{i,j} * EI_{i,j} * PE_{i,j} * LGE_{i,j};$$

usually, for the total absorption, the simple sum of the various absorptions is calculated on the basis of the building block approach.

$$K_{IMA} = \sum_{i=1}^n \sum_{j=1}^m (EI_{i,j} \cdot PE_{i,j} \cdot LGE_{i,j}) \cdot \gamma_{i,j} = \sum_{i=1}^n \sum_{j=1}^m EI_{i,j} \cdot \gamma_{i,j}$$

where:

- K_{IMA} = the capital requirement under the IMA;
- $\gamma_{i,j}$ = a fixed percentage, proposed by banks and accepted by Supervisory Authorities, on the basis of expected losses for each combination of business line and event type;
- $EI_{i,j}$ = the level of exposure indicator for the given business line and event type;
- $PE_{i,j}$ = the probability of a loss event for the given business line and event type; and
- $LGE_{i,j}$ = the average loss should a loss event occur for the given business line and event type.

2.3.2 Loss Distribution Approach

Potentially, the Loss Distribution Approach (LDA) can reflect better than the previous approach the actual risk incurred by the single banks. It differs from the previous one in the fact that the estimate of the unexpected losses is carried out directly and not in a mediated manner that is through the assumption of hypotheses concerning the possible relationship between expected losses and unexpected losses (which translated into the multiplying factor γ). For each business line and for each loss event, the bank must:

- estimate two probability distributions: (1) The frequency distribution of the loss event (PE) given a temporal horizon of one year; (2) The severity distribution of the loss upon the occurrence of the event (LGE);
- develop, on the basis of the two distributions mentioned, the cumulated distribution of losses;
- calculate the Value at Risk of said distribution; and
- sum the VaR calculated for each combination of business line/loss event so as to obtain the capital requirement with respect to operational risk or use techniques that keep into account the imperfect correlation among losses related to the various categories of events.

The bank is free to assume that the probability loss distributions of frequency and severity have different forms (e.g. Poisson and log-normal), or it can obtain the form of said distributions empirically. In particular, Poisson's probability distribution is particularly fit to represent the distribution of the amount of losses registered in a year, since the underlying hypotheses consist in a low probability that the event may occur and the independence of the variable amount of events from one year to another. The LDA will be analysed more in detail in Chaps. 3 and 4.

2.3.3 Scorecard Approach

The calculation of the capital requirement with respect to operational risk through the Scorecard Approach obliges the bank to:

- define capital requirement at the level of the whole institution, using estimate methods analogous to those used in the previous approaches;
- attribute the capital to the single business units according to the related risk profile, established on the basis of the result of the scorecards;
- identify a number of indicators capable of expressing particular types of risk within the single business lines;

- develop scorecards that reflect the risk of the single business lines and the effectiveness of the internal control system (capacity to reduce the frequency and severity of future operational losses);
- require for the personnel of each unit to fill in scorecards periodically (at least once a year);
- use the internal loss data to validate the results of the scorecards;
- submit the scorecards to the review of the internal control system; and
- adjust the capital requirement and review the allocation of the same along the various business lines on the basis of the results of the scorecards.

Therefore, the bank translates the qualitative assessments, resulting from a scoring process, into forecasting quantitative estimates, based on risk indicators tested and approved by the Supervisory Authority. In order to fall within the category of the AMA, said methodologies must be founded on solid quantitative bases and rigorous analyses of internal and external data. The determining element that emerges from said regulatory forecast is the acknowledgement, not only theoretical, of the fundamental role carried out by internal controls in Operational Risk Management. Said acknowledgement constitutes an effective incentive to improve an institution's internal control system.

The Supervisory Authority does not limit the choice concerning the methodological approach to use in calculating capital requirement according to an Internal Measurement Approach, although it subjects the use to the fulfilment of quantitative and qualitative criteria. The Authority does not impose any particular model of probability distribution of losses arising from operational risk. Actually, each bank wanting to adopt an advanced approach is free to choose among the many operational risk measurement methodologies (which will be presented in Chap. 3).

Initially, the adoption of the AMA can concern only several business lines, and it is nonetheless subject to a period of observation by the Supervisory Authority so that it can assess the credibility and correspondence of the risk management system to the activities carried out by the specific institution. In general, the capital requirement on

operational risks is given by the sum of the expected and unexpected losses, estimated through the calculation approach; it can be reduced through the use of insurance policies and other mechanisms of risk transfer within the limit of twenty per cent of the gross requirement. More in detail, the bank's use of an internal measurement system requires to estimate unexpected losses in a reasonable measure, on the basis of an integrated manner, of relevant internal and external loss data, of scenario analyses, as well as of the bank's specific factors related to the operational context and internal control system.

2.4 Data Collection

Regulation No. 575/2013 (CRR) allows banks to make use of the most sophisticated methods, that is the *Advanced Measurement Approaches*, based on four data categories of operational risk. Specifically, the four primary data sources are internal loss data (historical operational loss), external loss data (coming from external and consortia databases and used to deal with sparse nature of ILD, particularly for large or 'tail' losses), scenario data (used to fill the gap due to sparse ILD data and provide alternative forward-looking and a subjective view of the operational risk) and business environment and internal control factors (BEICF, typically consisting of risk and control assessments, KRIs and KCIs), where only the first data source is in SMA and the others are not. As mentioned, it is an integrated data collection (Fig. 2.2).

According to the regulatory ratio, said data collection process must be able to integrate more specifically:

- *Internal Loss Data*: said data represent the key component of developing a reliable and accurate system for measuring operational risks. The collection of internal loss data,¹ unavoidable condition for the development and functioning of the system, allows financial intermediaries to use the data on several fronts: as validation tool of the latter's inputs and outputs; as basis for empirical risk estimates; and as element connecting loss events with decisions made with reference to risk management and control. The internal loss data mapping



Fig. 2.2 An integrated data collection: four data categories. *Source* Authors' elaboration

is referred to not only the losses gross of recoveries, but also the recoveries amounts, the date on which the event occurred, if available, as well as identification and accounting. In order to calculate the capital requirement, the bank identifies fit minimum thresholds of loss, keeping into account the characteristics of operational risk classes. The thresholds identified must not entail the exclusion of significant loss data and must not condition the reliability and accuracy of operational risk distributions and measures. The bank must include in the mapping all the operational loss data identified above the thresholds. In exceptional cases, it can also be possible to exclude data that would determine a distorted and inconsistent representation of the bank's operational risk profile. The system for measuring operational risks must be based on a minimum five-year period of observation of the internal data. This period is reduced to three years when the advanced approaches are launched for the first time. The bank defines opportune classification criteria of the internal data to be attributed to the business lines and the loss events identified.

- *External Loss Data*: said data mainly come from consortia sources (information provided by a set of banks and other financial intermediaries), market sources (archives acquired by suppliers of the sector) or processed internally on the basis of information collected. The correct mapping and classification of all risk events occurred and related

are the prerequisite for carrying out analyses correctly and the consequent planning/realization of interventions useful for improving the Operational Risk Management process. The key critical aspects of the loss data collection, ascribable to its limited covering and weak predictive nature, justify the fact of supporting this component with external data and experts' estimates. Integration is even more necessary for major events, called also *black swan events* (low-frequency, high-impact, LFHI), increasing the limit connected both to the high level of context dependency and to the scarcity of data available. The gaps in a bank's historical experience can be filled, at least in part, by drawing information from consortia databases: these, besides constituting a useful methodological model of reference for organizing internal data collection, fill the asymmetries in a large amount of observations. Upon prior implementation of scaling formulas based on a linear factor that allows to adapt the data of the external sample to the probability distribution of the single bank, the LFHI loss events can fall within the latter, allowing to investigate the tail distribution. For statistical analyses to be accurate and extreme events to be relevant, the temporal horizon of the external data collection must be broad; the range of intermediaries must be sufficiently wide; and the data must be homogeneous by defining the loss to be reported, by developing a decisional tree for risk events and by mapping the business lines. Most banks are members of a data collection consortium²: each member reports internal loss events using a standard format and has access to other banks' loss events; the standard format includes loss size, Basel event type and business line, and date of loss; the motivation for using ELD is its size; and difficulty comes from potential disparities between banks' risk profiles and differences in loss frequencies and severities.

- *Scenario analysis*: it is necessary to integrate the scenario analysis in the operational measurement system, especially when the bank is exposed to high-severity losses, although not very frequent. Scenario data must be reliable and consistent with the bank's risk profile. Therefore, generating data must be exempt as much as possible from elements of subjectivity and distortions. In order to reach

said aim, the bank can adopt the following techniques: (i) it can set criteria for choosing the risk classes to which to apply the scenarios so as to identify informative sources; (ii) it can involve a plurality of experts, internal or external the bank, who will participate in the process for defining scenarios; and (iii) it can compare internal loss data and external loss data with the results of the scenario analyses so as to verify their capacity to identify the actual operational risk profile. External data can be used for scenario assessment. Some selected external losses can be added to internal losses; a joint data set is fitted with a severity. An approach is to fit internal and external losses with distributions and take a weighted average of these distributions: Parameter Averaging; Quantile Averaging with Constant Weights; and Quantile Averaging with Non-Constant Weights.

- *Business Environment and Internal Control Factors (BEICF)*: as mentioned, these factors are important for establishing the bank's risk profile. In fact, the aim of the BEICF is to incorporate in the estimate of capital requirement a *forward-looking* elements capable of reflecting as quick as possible the improvement or worsening of the bank's risk profile following changes that can occur in business lines, human resources, technological and organizational resources and the internal control system. In other words, apart from the possibility to use loss data (actual or based on scenario analyses), an overall operational risk assessment methodology must allow to identify the business environment and internal control factors, since these can modify the institution's operational risk profile. By using these factors, risk assessment should result more *forward-looking* and represent the status of the actual factors directly. They should also foster the alignment of the institution's assessment of needs with the aims of risk management, and lastly, they should promptly identify improvement or worsening in operational risk profiles. In the light of the above, each factor is identified on the basis of the predictive capacity of exposure to operational risks. In particular, the BEICF are expressed in the form of Key Risk Indicators (KRIs), Key Performance Indicators (KPIs) or Key Control Indicators (KCIs) as highlighted in Table 2.2.

Table 2.2 Business environment and internal control factors. *Source* Authors' elaboration

BEICF	
KRI	This is a metric of a risk factor. It provides information on the institution's level of exposure to a given operational risk at a particular point in time. KRIs are useful tools for business line managers, for the senior management and the Board of Directors as they help monitor the level of risk taking within an activity or institution, with regard to risk appetite
KPI	This indicator measures performance or the achievement of targets. Key Control Indicators, usually referred to as KCIs, are metrics that provide information on the extent to which a given control system is meeting its intended objectives. Failed tests on key controls are natural examples of effective KCIs

The BEICF can be used by institutions as a means of control for tracking changes in exposure to operational risk; they may play a more dominant role in the risk measurement system. When selected appropriately, these indicators should flag any likely change or the impact of an occurring risk. For financial institutions that use AMA, Internal Measurement Approaches, KPIs, KRIs and KCIs are advisable metrics (Vinella and Jin 2005) to capture BEICF. While the definition of BEICF differs among jurisdictions and in many cases is specific to individual organizations, these factors must be risk sensitive; provide management with information on the institution's risk profile; represent meaningful drivers of exposure which can be quantified; and be used across the entire institution.³ Incorporating BEICF into Operational Risk Modelling is a reflection of the modelling assumption that operational risk can be viewed as a function for controlling the environment.

2.5 AMA Methodologies: LDA

An appropriate system for measuring operational risks should be based on a preventive mapping of causal factors from which to ascribe historical losses reported by the bank and other banks, in the light of which it is possible to create an adequate database. Said database results essential for reaching an efficient operational risk measurement.

As we underline before, under the AMA, one of the most used methods to calculate operational loss distribution is the LDA approach (*Loss Distribution Approach*)⁴ which breaks down the aggregated losses into frequency and *severity* components. After estimating the frequency and severity distribution of loss events and, therefore, the aggregated distribution of losses, the determination of the VaR should lead to estimate the maximum potential loss that a business unit and, subsequently, the entire bank (summing the VaR of the single business unit) may undergo in a specific holding period and at a certain level of confidence. The LDA presents the advantage of a more accurate and consistent measurement of the institution's exposure to operational risk, because developed ad hoc for the single bank; this does not mean, though, that it produces a lower capital requirement compared to the other methodologies for calculating capital requirement. Results may be lower or higher than any result obtained with the *Basic Indicator Approach* or with the *Standardized Approach*.

Under the LDA, for each business line and for each loss event, the bank must:

- estimate two probability distributions: (1) The frequency distribution of the loss event (PE) given a holding period (*frequency* distribution); (2) The severity distribution of the loss upon the occurrence of the event (*severity* distribution). The hypothesis normally adopted is that loss data are independent and identically distributed, and that the useful information contained in the historical series is caught completely by two fundamental dimensions associated with the loss event: frequency and severity;
- develop, on the basis of the two distributions mentioned, the cumulated distribution of losses. To determine the aggregated loss distribution function through analytical methods is an extremely complex operation. The simplest solution for determining loss distribution consists in recurring to simulation techniques. The development of the severity and frequency distribution of loss events for each business line cannot be carried out exclusively through statistical techniques and traditional distributions;

- calculate the Value at Risk of said distribution on an annual holding period as to the interval of confidence chosen by the bank (consistently with the choices defined in its Risk Appetite Framework⁵); and
- sum the VaR calculated for each combination of business line/loss event so as to obtain the capital requirement with respect to the operational risk or use techniques that keep into account the imperfect correlation among losses related to the various categories of events (Fig. 2.3).

This different phases will be discussed synthetically in the below paragraphs but will be deepened in the Chaps. 4 and 5.

2.5.1 Frequency Distribution

Frequency distribution is the distribution of the amount of operational losses occurred in the holding period. To develop the frequency distribution of a loss event means to measure the number of times in which the event type occurred in different periods within a business line and to describe the probability according to which that event will occur $1, 2, \dots, n$ times in the same period of time (e.g. one year).

For this distribution, only internal loss data are used because they are more fit to estimate the frequency of a given loss event and represent the bank's characteristics.

The bank is free to assume that the probability frequency and severity loss distributions have different forms (e.g. Poisson and log-normal), or it can obtain the form of said distributions empirically. Frequency is defined as the probability distribution of the number of operational losses during a year. To develop the frequency distribution of a loss event means to measure the number of times in which the event type occurred in different periods within a business line and describe the probability according to which that event will occur $1, 2, \dots, n$ times in the same period of time (e.g. one year).

Often the Poisson distribution⁶ is used in frequency distribution, as it well represents the number of events that can occur in a given period of time. The estimate is carried out through the moments method, and the

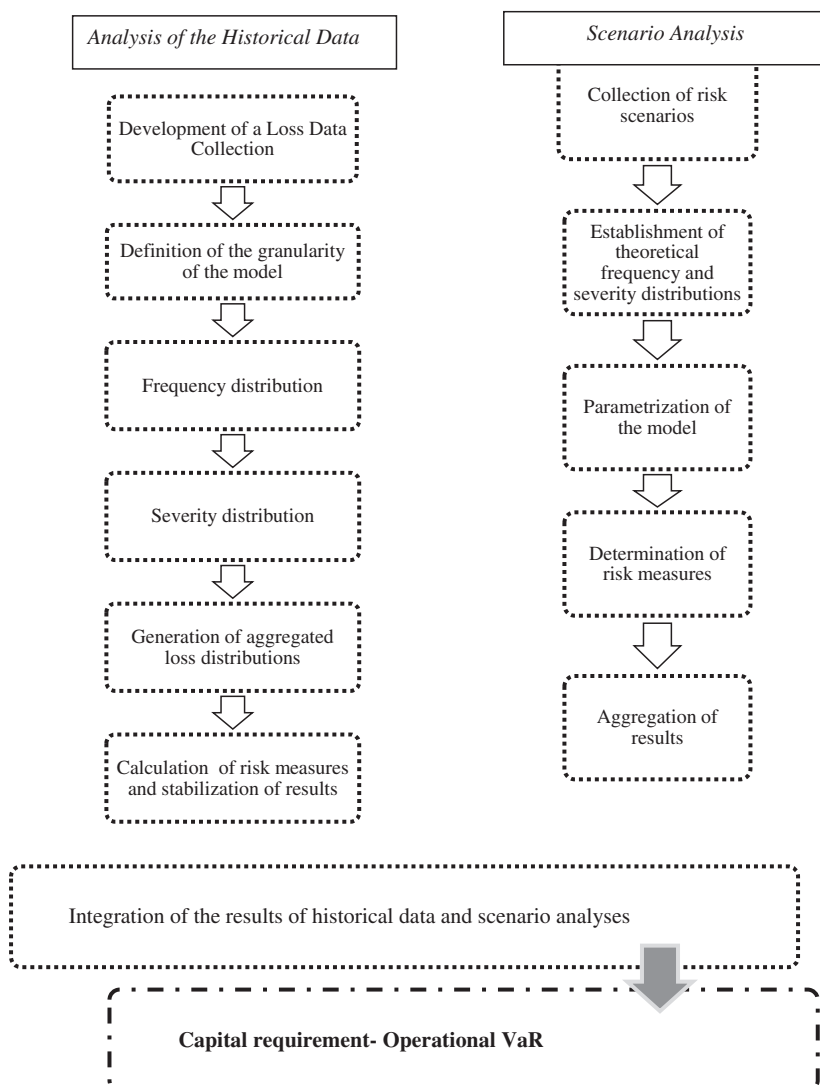


Fig. 2.3 Process for calculating the capital requirement with respect to operational risk. *Source* Authors' elaboration

fitting of the data with reference to the chosen distribution is verified through the Q-Q Plot and other quantitative methods. In general, the Poisson distribution well approximates the frequency of many events. However, it tends to overestimate the probability that events may occur few times (e.g. in a day) compared to the probability that they may occur many times, since the events considered within operational risk are rarely independent. Therefore, it is easy that if one event occurs, another one will occur as well.

Besides showing a trend compatible with the dynamics of the operational losses observed, another advantage of the Poisson function is that it estimates a single parameter, coinciding with both the average and the variance. Other distributions used are the binomial and the negative binomial, in particular when the data observed produce significant differences between the average and variance estimates.

At this point, it is important to observe that the crucial moment for a bank when implementing an LDA is when it has to make a good estimate of the severity distribution. The reason for which said moment is crucial lies in the impact that the mentioned loss events could have. Said events are present in the right tail of the severity distribution, and despite often being low-frequency events, they can have a relevant impact on the absorption of regulatory capital. It is for this reason that given the limited experience of tail events in financial institutions' internal data, the supervisory framework has required with reference to operational risk the incorporation of extra data, that is external data or data coming from scenario analyses.

2.5.2 Severity Distribution

Severity distribution represents the density of the probability of losses arising from a single operational event. To develop the severity distribution, it is necessary to measure the impact of the amount of losses deriving from the event type considered in a business line and establish the probability according to which the loss deriving from said event type will assume specific monetary values. The calculation of the first four moments of the sample (arithmetic average, variance, skewness index

and kurtosis index) allows to establish whether the data sample is distributed normally; whether the distribution presents a positive or negative asymmetry; and whether it is hypernormal or hyponormal (many distributions of operational losses are asymmetric and leptokurtic and have heavy tails). Dividing the amount of losses into value intervals, it is possible to observe the frequencies with which data fall within each interval and verify whether the distribution has heavy tails. The type of mathematical function usually used in order to represent the distribution of the phenomenon observed (i.e. to substitute the empirical curve with a theoretical curve that answers a mathematical function) consists of a continuous distribution; this is unlike the distributions candidate to approximate frequency loss distributions which can be discrete, if a small amount of events occur in a period of time, and continuous only if a sufficiently high number of events occur in each period of time.

After identifying the proper distribution for representing the data, a series of formal tests are carried out so as to verify the conformity of the sample of observations with the theoretical distributions selected (*goodness-of-fit* test). The conformity tests have the aim to assess the overall fitting (of the distribution average, variability and form) of the observations of a sample to a theoretical model, that is to verify that the data observed come from the distribution selected with the parameters estimated.

An important property of the density function is that it cannot assume negative values; it will have a single tail: the right tail. Generally, severity is divided into two parts: the body and the right tail. This distinction is made principally because the typologies of distributions used for the body (such as the log-normal) do not allow to identify the extreme loss events (those of the right tail).

2.5.3 Body Severity Distribution

The body severity distribution generally refers to internal losses, that is losses which refer to the data observed within the bank, connected to the institution's operational model. The body distribution of each single loss event follows a specific distribution that can be modelled, for instance, with a *log-normal distribution*.⁷

Generally speaking, ‘adjustments’ are carried out in the body of the severity distribution making it a cut log-normal distribution, since the bank’s risk management, in defining ‘*internal loss data*’, sets threshold data for each risk class, while operational losses under the threshold are not taken into consideration in the data set. This means that the distribution is cut in correspondence with the threshold. It can be assumed, in general, that the losses not observed under the threshold follow the same loss distribution observed above the threshold. Consequently, all this implies the estimate of conditioned frequencies and severities based on loss events above the threshold.

As it can be well understood, to set a threshold below which loss data are excluded from the data set, implies the risk not to keep into account loss data that can turn out to be important. Hence, as suggested even by the regulatory framework, cut models are used as well as shifted models which do not envisage any assumption concerning a loss distribution not observed below the threshold. In fact, frequency and severity parameters are estimated assuming that the losses observed follow a particular distribution after a shift. In other words, the aim of the shifted model is not to understand the behaviour of losses below the threshold. However, if it were necessary to investigate the case, said losses would not follow the same loss distribution above the threshold.⁸

2.5.3.1 Estimate of the Log-Normal Distribution Parameters

In order to estimate parameters of the body severity distribution $(\hat{\mu}, \hat{\sigma}^2)$, the most fit methodology is that of the *maximum likelihood estimation*—*MLE*, which allows to establish estimators that are considered better than those established with other methodologies.

The MLE method starts from what is defined *likelihood function*, which indicates the probability density (in the case of continuous variables) to observe a fixed sample (the operational losses present in the data set), upon the varying of parameter Θ .⁹

$$L(\Theta; x_1, x_2, \dots, x_n) = f_x(x_1, x_2, \dots, x_n) = \prod_{i=1}^n f(x; \Theta)$$

where:

- L is the likelihood function;
- f_x is the density probability function of X ; and
- Θ is the vector of the parameters.

In the likelihood function, the sample data are known, while the parameter Θ is not. It is important to highlight that among various values of Θ , the greatest one is to be preferred, that is the most likely one, thus tending to the value of Θ that maximizes the likelihood function.

This leads to the maximum likelihood which is obtained choosing a Θ such as to maximize the likelihood function L .

$$\bar{\Theta} = \max L(\Theta; x_1, x_2, \dots, x_n)$$

The value of Θ , as mentioned, is not known; hence, in order to establish it, it is necessary to proceed either analytically or through specific software. In the specific case of the cut log-normal distribution, it is not possible to reach a clarification of the maximum likelihood estimators for analytical reasons. Therefore, it is necessary to recur to specific methodologies.

2.5.3.2 Goodness-of-Fit Test of the Distribution

Once defined how to distribute the body severity and once estimated the parameters with the MLE method, it is necessary to make sure that the distribution chosen—in this case, the log-normal—fits the loss data at disposal at the best. To assess the goodness of fit, it is possible to start by using a graphic method, the *Quantile-Quantile Plot* (Q-Q Plot). The latter allows to assess, through graphic representation, whether the loss data set at disposal fits well with the theoretical distribution chosen.

If there is correspondence between the two distributions—the theoretical distribution and the actual distribution of loss data—it means that the theoretical distribution chosen does not underestimate or overestimate the actual loss data distribution.

However, this graphic method is not sufficient to verify alone the goodness of fit of the actual data to the theoretical distribution. Therefore, it is generally supported by more precise quantitative methods. These methods refer to statistical tests that verify whether or not the loss data at disposal are distributed according to the theoretical distribution chosen.

The statistics mostly used for these tests, and in the specific case of the cut distributions, are Kolmogorov–Smirnov and Anderson–Darling. The best fit is represented by the distribution that presents the lowest values of statistical tests (the values of the Anderson–Darling test are preferred). Generally speaking, the expectancy is that the traditional distributions, despite passing the goodness-of-fit tests, do not approximate the tail severity distribution adequately. The operational risks, especially if a specific analysis for event type is not carried out, give place to a large number of losses of small amount and a very low number of ‘extreme’ losses. The graphic and formal tests could lead to refuse all the traditional distributions since the ‘body’ and the ‘tail’ of the data do not always come from the same distribution. If none of the candidate distributions seems to approximate well the severity data of the loss sample, in particular starting from the higher quantiles, it will be necessary to recur to Extreme Value Theory models.

2.5.4 Tail Severity Distribution

Losses beyond the body, thus the right tail distribution, are generally losses related to data not observed within the bank, often characterized by low frequency and, therefore, identified externally or through scenario analyses. To outline the boundary between the body distribution data and those of the right tail, the bank’s risk management must set another threshold starting from which the right tail distribution will have origin, and starting from which the external data of operational loss or scenario analysis will be used. The choice of this parameter is not easy: it is necessary to choose a large enough threshold in order to consider extreme losses that truly are such; at the same time, though, if its

value is exceedingly high, there would be a less number of observations to estimate the parameters of the distribution of said losses.

The choice of this parameter is very important also because, as we will see further on, the analyses carried out to evaluate the goodness of fit of the right tail depend on said choice.

These tail data are followed by a distribution different from that of the body, with the intent to give more weight to extreme losses, as they affect the regulatory capital more.

To model the tail severity distribution, it is necessary to start from the theory of extreme values which allows, through specific methodologies, to define the distribution that better describes the behaviour of extreme values. The EVT models (as we explain better in the subsequent chapter) allow to forecast, at a given level of confidence, the possible losses generated by catastrophe events, which occur rarely but whose impact is very high. Therefore, said models allow to identify the economic capital to allocate to a particular business line so as to defend it from a possible operational catastrophe. Moreover, the EVT allows to estimate in an optimal way the tail loss distribution through a generalized distribution, allowing to overcome the limits deriving from the difficulty to assume the form of the underlying distribution generated by the unavailability of wide historical series of data. Among the methods used, there are:

- *Block Maxima*: this method considers the maximum values that the operational loss variable assumes in subsequent periods of time, for instance, months or years. These observations constitute extreme events, also called Block Maxima.
- *POT (Peaks over Threshold)*: this method estimates the tail of the probability distribution of operational losses using only the data that exceed a high-value threshold, regardless of when they occurred. The POT¹⁰ is based on the fact that excesses of losses beyond a certain threshold of high value are distributed according to a Generalized Distribution of Pareto (GDP). The latter is a distribution used often, exactly as in our case, to model tails of other distributions since it allows to give more weight to extreme values falling within the tails.

As already mentioned for the body severity distribution, even in this case, it is possible to verify the trend of the data at disposal with the theoretical distribution chosen, through graphic methods such as the Q-Q Plot, always with the support of quantitative methods such as those already mentioned. In this case, though, it is also possible to test the adaptability of the data, verifying how good the estimates of the distribution parameters are upon the varying of the threshold u . In fact, as mentioned, the choice of the parameter u is very important even to evaluate the goodness of fit chosen for the right tail.

2.5.5 Severity and Frequency Convolution

After modelling the frequency distribution and the severity distribution, plus after estimating the parameters of said distributions and testing the adjustment of the loss data at disposal to the theoretical distributions chosen, it is possible to proceed with the convolution of the two distributions. Generally speaking, it is extremely complex to determine said distribution through analytical methods. The simplest and most widespread solution consists in using the Monte Carlo simulation. The convolution is carried out with the Monte Carlo method, which refers to a family of simulation methodologies, created for very different purposes from our scope of implementation. The Monte Carlo simulation is a random simulation based on an algorithm, from which the annual aggregated loss related to a class of operational risk is obtained as follows:

$$S = \sum_{i=1}^N s_i + s'$$

where:

- S is the annual aggregated loss per class of operational risk;
- N is the number of losses simulated by the frequency distribution;
- s_i is the amount of a single loss simulated above the threshold H ; and
- s' is the empirical average of the annual aggregated losses below the threshold.

In order to develop the aggregated distribution, it is necessary to start from the assumption that all events are mutually independent; that the cost of every ‘accident’ is distributed identically; and that the frequency distribution and the severity distribution are independent. These are limiting hypotheses that nullify the validity of the model despite simplifying the computation moment of the measurement of the capital at risk for operational losses.

Once established the annual aggregated losses for each class of risk, it is necessary to proceed aggregating them among each other assuming a perfect linear correlation or other correlation structures.¹¹ In case of a perfect linear correlation, it is necessary to proceed simply summing the annual aggregated losses for each risk class, obtaining a *multi-varied distribution*, which is a distribution deriving from a vector of random variables. Therefore, it is a distribution with higher dimensions.

In order to pass to the aggregation of distributions related to each risk class, copulas are used which, as formulated by Sklar’s Theorem,¹² are simply multi-varied distributions that allow to reach the joint distribution on which the VaR can be established (see Chap. 3).

2.6 Calculation of the Operational VaR

The VaR is calculated once obtained the annual aggregated distribution of the operational losses for each event type. The operational VaR derives from the combination of severity models and frequency models: it is the result of a loss interference process and requires different tests that certify its reliability.

As known, the VaR metrics have a consolidated literature and operational practices concerning market risk, but they are fit to be moved, not without difficulty, to great part of quantifiable risks, therefore also to operational risks. However, there are differences between Operational VaR and Market VaR:

- The operational loss probability distribution cannot be modelled with the normal distribution as with the market risk distribution;

- The VaR market models do not consider the frequency of events because the assumption is that the prices of the activities follow a continuous stochastic process (stock market are continuous on a day). Operational losses, instead, follow discrete stochastic processes, that is they are countable in a certain period (an operational event occurs n times per day). As mentioned, the stochastic process on which the operational risk is based is the Poisson process.

Although the internal methods for measuring operational risk are very expensive to implement, many banks, especially the large ones, prefer internal models to the other two methods proposed by the regulatory framework because, generally speaking, they allow to allocate a lower capital estimate. In fact, internal approaches are developed ad hoc, on the basis of specific characteristics of the business model and of the bank's related operational losses. Therefore, they allow to establish a more contained capital requirement compared to the other two regulatory approaches. Hence, there is a clear trade-off between the complexity of the measurement models and the regulatory capital requirement (Fig. 2.4). Moreover, the Basic Indicator Approach and the Standardized Approach quantify the operational risk without identifying the events or the cause of losses and are a disincentive to report losses (because they do not require a data collection). Moreover, they capture both the expected loss and the unexpected loss, when the

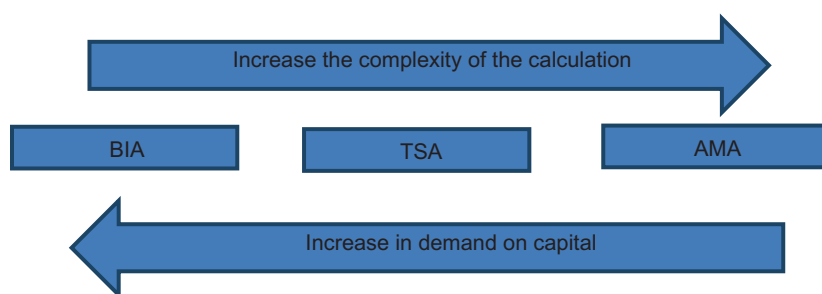


Fig. 2.4 Trade-off between calculation complexity (and greater implementation costs) and saving in terms of AMA's capital allocation. *Source* Author's elaboration on Valová, I. (2011). 'Basel II approaches for the calculation of the regulatory capital for operational risk'

regulatory capital should only reflect the unexpected loss. In this perspective, BIA and TSA induce risk-taking behaviours, failing to achieve the Basel Committee's objectives of stability and soundness within the financial institutions. Moral hazard and other unintended consequences are more risk-taking, without the possibility of capital reduction for better risk management, in the face of increased funding costs due to the rise in capital. It is predictable that financial institutions will raise their risk-taking to a level sufficient enough to pay for the increased cost of the new fixed capital. A financial institution mechanically increases risk appetite (Jarrow 2008).¹³

Nonetheless, BEICF (a key source of the Operational Risk Data) are not included in the SMA and BIA and cannot easily be incorporated with the SMA framework, even if there were the desire to do so, due to the level of granularity implied by the SMA. All this makes capital calculations less risk sensitive. Furthermore, the lack of scenario-based data incorporated in the SMA model makes it less forward-looking and anticipatory as an internal model-based capital calculation framework.

This effect goes against the Basel Committee's objective of a safe and more resilient financial system. The greatest advantage of these approaches is that they do not require great efforts in collecting data and, therefore, in the actual operational risk assessment. The Advanced Measurement Approaches quantify operational risk by identifying loss events (data collection). They attempt to explain the mechanisms that govern the forming of operational losses and imply a process for managing operational losses as prescribed by the operational regulatory framework.

2.7 Operational Requirements to Be Eligible for AMA Methodologies

Competent Authorities authorize banks to use the Advanced Measurement Approaches—based on the single institution's operational risk measurement systems—upon the fulfilment of qualitative and quantitative requirements, as provided for by Articles 321 and

322 of the Regulation and when the institution meets the organizational requirements laid down in Directive 2013/36/EU (CRD IV). According to the mentioned requirements, for the methodologies in object to be validated, the following aspects are taken into consideration: the effectiveness of the operational loss management process, control procedures, reports, the organizational structure and not the sophistication of the statistical-mathematical measurement engine of operational losses, as it may be erroneously thought. Seemingly, this is the direction undertaken also by the new operational supervisory measures that have introduced the new Standard Approach, as we will highlight in Chap. 5. The idea underlying the regulatory framework seems to be that the use of internal models is allowed, regardless of the sophistication of the model, if there is an organized and integrated process for measuring, managing and controlling operational losses.

With reference to *organizational requirements* (Fig. 2.5), the bank must comply with what provided for by the Authorities as regards internal controls and the Operational Risk Management system, as analysed hereafter in detail.

With reference to the **internal control system** (Fig. 2.6), Supervisory Authorities have established that banks wanting to obtain the validation

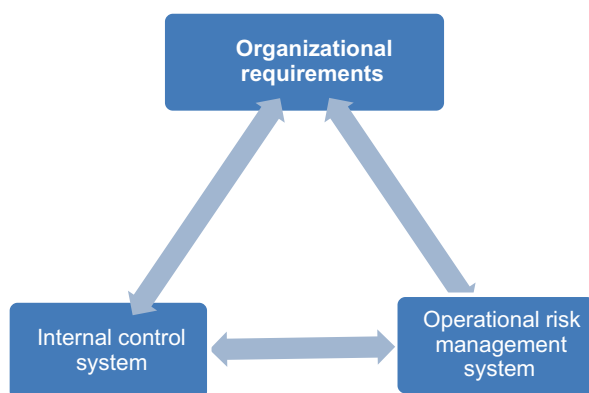


Fig. 2.5 Organizational requirements to be eligible for AMA methodologies.
Source Authors' elaboration

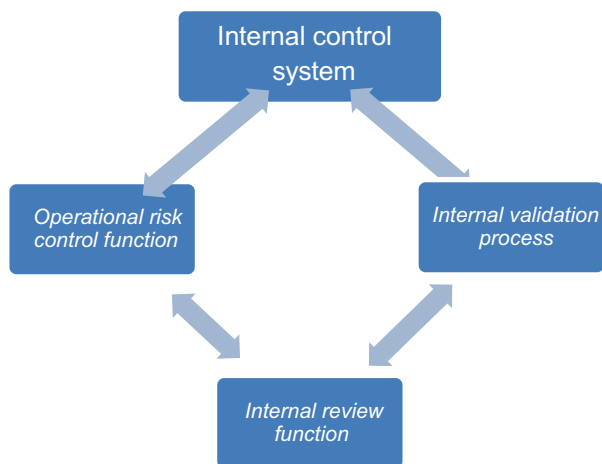


Fig. 2.6 Internal control system. *Source* Author's elaboration

of AMA methodologies must have an operational risk control function, an internal validation process and an internal review function.

In particular, the Authorities require for AMA banks to set up:

- a. an *operational risk control function* in charge of planning, developing and maintaining: Operational Risk Management and measurement systems, the data collection and preservation system, the reporting system and the operational risk profile assessment; it must also be able to determine the capital requirement on operational risks. This function can involve the bank's various structures and make use of resources specialized in Operational Risk Management and measurement methodologies. It must periodically inform the institution's bodies on the activities carried out and related results.
- b. an *internal validation process*, that is a set of procedures and activities aimed at assessing the quality of the Operational Risk Management and measurement systems, as well as their compliance over time with regulatory measures, with the company's needs and with the evolution of the market of reference. This process verifies the reliability of the calculation of the capital requirement and ascertains that the measurement system is adequate. The results of the validation process

must be adequately documented and subject to internal audit, to other structures or functions involved in the Operational Risk Management.

- c. an *internal review function*, that is a function that carries out periodical verifications on the Operational Risk Management and measurement systems to assess their effectiveness and compliance with the qualifying criteria. In particular, it verifies the internal validation process and the actual use for managerial purposes of the operational risk measurement system. Moreover, it must keep the institution's bodies informed on the activities carried out and related outcomes producing a yearly report aimed at illustrating the activities carried out and highlighting the critical aspects and the corrective interventions to be implemented.

At the same time, the Authorities require for AMA banks to create an Operational Risk Management system meant as a structured set of processes, functions and resources for identifying, assessing and controlling operational risks for the prevention and mitigation of actual risks.

According to what established by the Regulator, the Operational Risk Management system, it will be characterized by:

- the data collection and preservation system,
- the reporting system and
- the managerial uses of the operational loss measures (Fig. 2.7).

With reference to the data collection and preservation system, the bank must organize it in such a way that it is fit to assure the effectiveness of the management and measurement systems. Moreover, it must enable to fulfil the requirements of completeness, reliability and data updating by developing adequate informative systems capable of assuring information integrity, privacy and availability, as well as periodical verifications on the data collection and preservation system.

Likewise, the organization of a *reporting system* is aimed at assuring prompt information on operational risks to the institution's bodies and those responsible for the organizational functions involved. The most relevant information is that which concerns loss data and related



Fig. 2.7 Operational risk management process. *Source* Author's elaboration

recoveries, the evolution of factors of the operational context and the internal control system such as to modify the operational risk profile, the other areas of vulnerability and related actions for the prevention and mitigation of operational risks.

One of the essential elements of Operational Risk Management is the *managerial use of the measurement system (use test)*. The operational risk measurement system must result strictly integrated into the decisional processes and in the bank's risk management process. It must not be confined to a mere experimental laboratory of operational loss measurement. Moreover, it must not be used only to determine capital requirement, but must aim at strengthening the Operational Risk Management system, so as to improve business processes and the internal control system in its whole. In fact, the bank can use the AMA methods for calculating the capital requirement only as long as the operational risk measurement system is used for managerial purposes.

Once the internal approach has been validated, the Supervisory Authority subjects it to an initial monitoring period so as to establish whether the methodological approach is credible and appropriate. The internal measurement system must estimate, in a reasonable measure, unexpected losses on the basis of a combined use of the four components previously described and must serve as decisional support for the allocation of the economic capital to all business lines. From the regulatory viewpoint, although an internal methodology has not been explicitly prescribed, a set of both qualitative and quantitative conditions have been identified. First these were provided for, by Basel II, and currently, redefined in the CRR.

The *qualitative requirements* (Article 321 of CRR) described by the European laws, although providing less details, are more or less similar to those provided for by the BCBS and are as follows:

- an institution's internal operational risk measurement system shall be closely integrated into its day-to-day risk management processes;
- an institution shall have an independent risk management function for operational risk;
- an institution shall have in place regular reporting of operational risk exposures and loss experience and shall have in place procedures for taking appropriate corrective action;
- an institution's risk management system shall be well documented. An institution shall have in place routines for ensuring compliance and policies for the treatment of non-compliance;
- an institution shall subject its Operational Risk Management processes and measurement systems to regular reviews performed by internal or external auditors;
- an institution's internal validation processes shall operate in a sound and effective manner; and
- data flows and processes associated with an institution's risk measurement system shall be transparent and accessible.

The *quantitative requirements* (Article 322 of CRR) perfectly refer to those provided for by the BCBS, but they are organized on the basis of

operational risk process measurement, internal data, external data, scenario analysis and BEICF (see Table 2.3).

The main elements of differentiation between the European directive and the Basel II Accord consist in the scope of implementation that is extended not only to bank institutions but also to investment enterprises, as well as in the request to calculate the capital requirement at the level of each single credit institution of the group besides the consolidated basis.

2.8 In Addition to AMA Methodologies: Operational Risk Management

The Basel Committee has highlighted that internationally active banks and banks with significant exposures to operational risks should use a methodology more appropriate to their risk profile and with a higher sophistication level than the Basic Indicator Approach.¹⁴ However, the Advanced Measurement Approaches are characterized by a greater complexity not only at technical level but also at organizational and procedural level. In fact, they are based on the analysis of the single processes of each business unit so as to identify, classify and assess all the risks to which the institution is exposed. Indeed, they allow the bank to have an exact understanding of the real operational risk factors related to the institution's business.

Therefore, internal models do not involve only the bank's modeling activity, but they are also an issue related to databases, governance, internal control system, reporting and especially internal risk culture. And, in extreme synthesis, they are an issue related to process, procedures, organization, control systems and reporting; in other words, they are not only a measurement tool. Moreover, it is the efficient integration of all these elements that make the bank efficient and capable of producing value (also) in measuring and managing operational risks.

In this perspective, the operational risk measurement is only one of the moments of a complex process organized at various levels. It is a process that involves internal and external communication, a system

Table 2.3 The quantitative requirements provided for by the CRR. *Source* Authors' elaboration on Article 322 (CRR)

Operational risk process measurement

- The bank must calculate the capital requirement by summing expected losses and unexpected losses, unless the expected losses are not adequately estimated in the internal operational practices
 - The operational risk measurement system shall include the use of internal data, external data, scenario analysis and factors reflecting the business environment and internal control systems
 - The advanced measurement approach must be capable to identify potential high impact loss events and reach robustness standards consistent with a confidence level of 99.9% over a period of one year. An institution's risk measurement system shall capture the major drivers of risk affecting the shape of the tail of the estimated distribution of losses
 - The bank is permitted to consider correlations concerning operational losses among single operational risk estimates, as long as the systems for measuring correlations are sound, implemented with integrity and take into account the uncertainty surrounding any such correlation estimates, particularly in periods of stress. An institution shall validate its correlation assumptions using appropriate quantitative and qualitative techniques
-

Internal data

- The internal operational risk measurements must be based on a minimum historical observation period of five years. This period can be reduced to three years when the bank adopts an advanced measurement approach for the first time
 - The bank must be able to classify its internal loss data on the basis of business lines and event types and to provide these data to competent authorities upon request
 - The internal operational loss data must be exhaustive, that is they must include all relevant activities and exposures. The exclusion of activities or exposures is permitted, as long as the bank is able to prove that the said exclusion does not produce a relevant impact on the overall risk estimates. Moreover, with reference to the internal data collection, the institution must define adequate minimum loss thresholds
 - The data collected by the bank must concern gross loss amounts, an institution shall collect information about the date of the loss event, any recoveries of gross loss amounts, as well as descriptive information about the drivers or causes of the loss event
 - An institution shall have in place documented procedures for assessing the ongoing relevance of historical loss data, including those situations in which judgement overrides, scaling or other adjustments may be used, to what extent they may be used and who is authorised to make such decisions
-

(continued)

Table 2.3 (continued)

External data

- The operational risk measurement system must make use of pertinent external data, especially if the bank is exposed to losses which are not frequent but characterised by a potentially high severity. An institution shall have a systematic process for determining the situations for which external data shall be used and the methodologies used to incorporate the data in its measurement system
- The conditions and practices for using external data must be well documented and undergo periodical review

Scenario analysis

- In order to assess exposure to events of particular seriousness, the bank must also use scenario analyses carried out by experts. These assessments must be validated and reviewed periodically on the basis of a comparison with the actual losses incurred

BEICF

- An institution's firm-wide risk assessment methodology shall capture key business environment and internal control factors that can change the institution's operational risk profile
- An institution shall justify the choice of each factor as a meaningful driver of risk, based on experience and involving the expert judgment of the affected business areas
- An institution shall be able to justify to competent authorities the sensitivity of risk estimates to changes in the factors and the relative weighting of the various factors. In addition to capturing changes in risk due to improvements in risk controls, an institution's risk measurement framework shall also capture potential increases in risk due to greater complexity of activities or increased business volume

of incentives for those responsible of business and process, the ethical and value dimension of personnel management, the logical and physical structures of the institution's information systems and the procedures and processes for identifying, monitoring, reporting and managing operational risk.

Already in February 2003, the Basel Committee in the document *Sound Practices for the Management and Supervision of Operational Risk* highlighted several basic principles for managing operational risk, thus guiding national Supervisory Authorities when implementing the Second Pillar. In particular, after establishing roles and responsibilities to be given to the bank's governance bodies, the *Sound Practices* assign

precise responsibilities to the Supervisory Authorities with reference to the operational risk. In fact, Authorities are called to:

- require for all banks, regardless of their dimension, to develop an Operational Risk Management system compliant with the Committee's indications and adequate to the institution's dimension, complexity and risk profile. This system must allow to identify, assess, monitor and control/mitigate operational risks effectively in an overall risk management approach;
- constantly assess policies, procedures and practices adopted by the bank in Operational Risk Management. These assessments concern the effectiveness of the risk management process and the internal control system; the monitoring and reporting methodologies, including operational loss data and other risk indicators; the procedures for identifying a quick and effective remedy to criticalities and vulnerabilities; the quality of the operational and emergency continuity plans; the effectiveness of risk mitigation tools; and the overall capital adequacy with reference to the operational risk profile;
- assure that the institutions belonging to a group adopt an integrated and appropriate risk management system;
- require a constant reporting from the controlled subjects;
- encourage efforts aimed at developing risk management processes through the monitoring and assessment of the progress achieved and of future projects;
- assist the controlled subjects in activity planning processes with the aim to avoid that efforts are made towards developments resulted ineffective in other experiences;
- verify the adequacy of the minimum requirements and compliance with the conditions provided for as regards the adoption of operational risk Advanced Measurement Approaches (AMA). This verification is preventive, aimed at the issuing of the authorization to use advanced methods, and it is continuative so as to make sure that requirements are fulfilled over time; and
- assess the adequacy of the capital requirement resulting from the implementation of the Basic Indicator Approach and the Standardized Approach to represent the bank's operational risk

exposure, on the basis of comparisons with institutions that have comparable sizes and operativeness.

After a couple of years, BCBS (2011b) identified a new framework for Operational Risk Management process (*Principles for the Sound Management of Operational Risk* (PSMOR)).¹⁵ Said principles find their starting point and their direction of development in a solid operational risk culture promoted by the bank's strategic bodies and diffused transversally to all of the institution's organizational roles. Specifically, these eleven principles concern the institution's organizational culture, the framework adopted for managing operational risk, the governance and environment of the Operational Risk Management (Table 2.4).

By turning the above-mentioned principles into 'a system', banks can develop an appropriate 'environment' for Operational Risk Management which involves the institution's strategic top management, the Board and the senior management, whose awareness and commitment must set the correct path towards an effective ORM and an appropriate related culture. Several principles refer to the ORM in its various phases/activities: identification, evaluation, monitoring and mitigation/control. The implementation of the Sound Practices requires for banks to not only adopt business solutions—in terms of ad hoc structures, IT supports and business mechanisms—but also, as said, the promotion and development of an *internal operational risk culture*. It is up to the Board of Directors to promote a solid culture of operational risk governance within the bank. The Board of Directors and the senior management must establish a business culture based on a robust risk management that incentivizes employees' responsible behaviour. Moreover, they must assure an adequate training in ORM within the entire company pyramid.

In this perspective, Operational Risk Management must fall within a broader picture, characterized by the single institution's specific strategic and organizational choices. Risk management includes, generally speaking, the identification and assessment of risks, the verification that an adequate capital planning has been carried out, the implementation of corrective actions for mitigating risks and a process for providing information to the management and ownership. A sound internal

Table 2.4 Principles for the sound management of operational risk. *Source* Author's elaboration on BCBS (2011b)

Organisational culture

Principle 1: The Board must promote a solid risk culture within the bank.

Together with the senior management, it must establish an organisational culture based on a robust risk management that incentivizes employees' responsible behaviour. It is up to the Board and the senior management to assure the implementation of an adequate training in operational risk management for the whole company pyramid

Operational risk management framework

Principle 2: Banks must develop, implement and maintain an integrated framework in risk management processes. The Operational Risk Management framework used in each bank depends on various factors, such as the bank's nature, organisational complexity, size and risk profile

Governance—Board of Directors

Principle 3: The Board must establish, approve and review the framework periodically. It must supervise the senior management so as to make sure that procedures, processes and systems are implemented effectively at all decisional levels

Principle 4: The Board shall approve and review a statement concerning tolerance and operational risk appetite that describes the nature, types and levels of risk that the bank is willing to undertake

Governance—Senior management

Principle 5: The senior management must identify a clear, efficient and robust governance structure characterized by well defined responsibility lines that must be approved by the Board. Moreover, the senior management must implement and review policies, processes and systems for the management of the operational risk inherent all of the bank's production resources, activities, processes and systems

Risk management environment—Identification and assessment

Principle 6: The senior management must assure a correct identification and assessment of the operational risk inherent all of the bank's production resources, activities, processes and systems, so as to establish the full understanding of incentives and shades characterizing this particular risk category

Principle 7: The senior management must assure the existence of a procedure for approving all new products, activities, processes and systems that provide a complete assessment of operational risk

Risk management environment—Monitoring and reporting

Principle 8: The senior management must implement a process capable of monitoring the bank's operational risk profile and material exposure to losses. An effective reporting mechanism must be established at the level of Board of Directors, senior management and business lines so as to guarantee a positive and constructive operational risk management

(continued)

Table 2.4 (continued)

Risk management environment—Control and mitigation

Principle 9: Banks must promote a control environment that makes use of procedures, systems, internal controls and strategies of operational risk mitigation/transfer

Risk management environment—Business resilience and continuity

Principle 10: Banks must be provided with *business resiliency plans* and *e-continuity plans* so that they can operate on a continuative basis limiting risk of losses deriving from possible serious interruptions in their activity

Risk management environment—Role of information made public

Principle 11: Banks must produce documents providing information allowing stakeholders to assess the approach used in the risk management

governance is the basis for an effective Operational Risk Management. In this regard, the Committee has highlighted that the safest and most diffused practices within the sector are based on three lines of defence¹⁶: (1) The institution's management of business lines; (2) The institution's independent Operational Risk Management function; and (3) The institution's independent review of the Operational Risk Management framework adopted.

The Committee's Principles for the Sound Management of Operational Risk defines regulatory expectations for the management of operational risk. All internationally active banks should implement policies, procedures and practices to carry out an Operational Risk Management calibrated with their size, complexity, activities and risk exposure and seek continuous improvement in these areas as the industry practice evolves. In order to enhance ORM, the principles provide comprehensive guidelines regarding the qualitative standards that should be followed by large internationally active banks.

According to the authors' opinion, as mentioned, there is the need to structure an *Operational Risk Management Process* not only with reference to intermediaries that use internal models, but also to those that, although using alternative regulatory methods, produce/undergo relevant operational losses due to their business model. For those intermediaries, the lack of an *advanced measurement method* can be certainly counterbalanced by a process devoted to operational risks, proportioned to the complexity and size of the business model, capable of defining

roles and responsibilities of the business units involved in the process of operational loss management. They can also develop a control and reporting system devoted expressly to operational risks and structures, and a data collection process of internal and external losses, idiosyncratic and systematic, useful for a future development of internal measurement models. In this view, it is a process that follows an integrated logic, starting from a solid management culture of Operational Risk Management, a correct definition of operational risk governance.

However, even these guidelines (Table 2.3), similarly to the principles described in the previous Table 2.4, provide important and valid indications for the configuration of a process of *Operational Risk Management* carried out by institutions for which operational losses represent an important portion of the overall capital absorption (internal and regulatory one) due to the business model.

2.9 Supervision Operational Risk. From Sound Practices to the New SREP

The sound practices briefly mentioned above did not find great implementation in the bank industry, but they probably set the basis for the supervisory and surveillance activities that the Authorities will carry out within the new SREP (*Supervisory Review and Evaluation Process* configured by the guidelines EBA (2014)¹⁷ in accordance with the Single Supervisory Mechanism (SSM).

As known, the new SREP (implemented as of 1 January 2017) is based on various phases:

- Classification of the institution and periodical review of said classification; monitoring of key indicators;
- Business Model Analysis (BMA);
- Evaluation of the institution's governance and internal controls;
- Evaluation of risks that affect capital;
- Evaluation of risks that affect liquidity;
- Evaluation of the adequacy of the institution's funds;

- Evaluation of the adequacy of the institution's liquidity resources;
- Overall evaluation of the SREP; and
- Surveillance measures (and prompt intervention measures, if necessary).

By combining quantitative information and qualitative information, the Supervisory Review and Evaluation Process leads to evaluate each bank's overall exposure to risk, keeping into account mitigation factors (e.g. real guarantees) and the organizational risk control. In particular, the following elements are analysed more in depth: profitability and sustainability of the business model; the company's governance system and risk control; capital adequacy as to credit risks, market risks, operational risks and interest rates; and the institution's liquidity profile.

Each element is given a score equal to 1 or 2 (favourable area) or 3 or 4 (unfavourable area). Then, the Supervisor has the task to perfect the assessment, within fixed margins of discretionary power, keeping into account further information and personal experience. Moreover, as regards the capital adequacy and liquidity profiles, the bank's self-evaluation exercises are kept into consideration, in both normal and stressful scenarios. The average of the assessments given to the four elements constitutes the final SREP score. The latter is the basis for identifying the necessary regulatory measures: for instance, the mandatory review of risk management processes; internal controls or governance structures; limitations to profit distribution or capital restitution; and imposition of additional capital or liquidity requirements (Fig. 2.8).

Without prejudicing the Board's and senior management responsibilities in management and organization of activities or without indicating preferences for specific business models, the competent Authorities should carry out regular Business Model Analyses (BMA) in order to evaluate the operational and strategic risks, as well as establish: the economic sustainability (viability) of the institution's business model on the basis of the capability to generate acceptable profits during the following 12 months and the sustainability of the institution's strategy on the basis of its capability to generate acceptable profits on a minimum temporal horizon of 3 years, with reference to its strategic plans and financial forecasts.

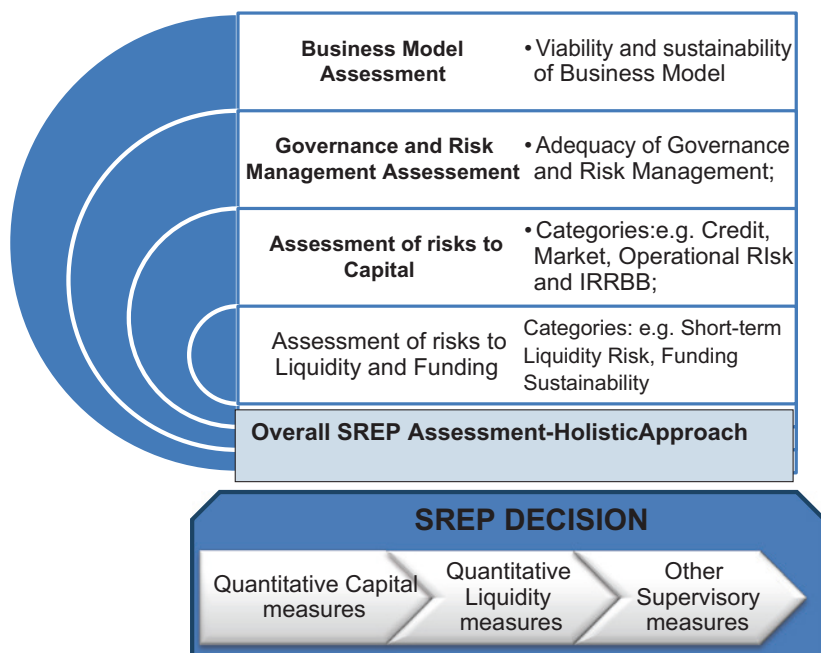


Fig. 2.8 The structure of the new SREP. *Source* Author's elaboration on European Central Bank (2016). 'SSM SREP Methodology Booklet'

Within the evaluation of risks that affect the capital, Supervisory Authorities should evaluate the operational risk throughout all of the institution's business lines and operations, taking into account findings from the assessment of internal governance arrangements and institution-wide controls. In conducting this assessment, they should determine how operational risk may materialize (economic loss, near miss, loss of future earnings, gain) and should also consider potential impacts in terms of other related risks (e.g. credit-operational risk, market-operational risk 'boundary cases'). Competent Authorities should assess the materiality of operational risk arising from outsourced services and activities, and whether these could affect the institution's ability to process transactions and/or provide services, or cause legal liabilities for damage to third parties (e.g. customers and other stakeholders).¹⁸

The Authorities should also consider that:

- **The reputational risk** is included under operational risk because there are strong links between the two (e.g. most operational risk events have a strong impact in terms of reputation). However, the outcome of the reputational risk assessment should not be reflected in the scoring of operational risk. Whereas, if relevant, it should be considered as part of the Business Model Analysis and/or liquidity risk assessment, since its main effects can be reductions in earnings and loss of confidence in or disaffection with the institution by investors, depositors or interbank-market participants.
- **The model risk** includes two distinct forms of risk, that is the risk connected to the underestimation of requirements as regards personal funds by the approved regulatory models (e.g. on the basis of the internal rating (IRB) for the credit risk) and the risk of losses related to the development, implementation or unfit use of other models by the institution due to decisional process (e.g. the pricing of derived products, the evaluation of financial tools and the monitoring of risk limits).

In evaluating the operational risk, the competent Authorities can use a classification of event types for the Advanced Measurement Approaches as mentioned under Article 324 of the Regulation (EU) No. 575/2013 (as indicated in the Commission's delegated regulation issued pursuant to Article 312, paragraph 4, of Regulation (EU) No. 575/2013). This allows to obtain a clearer view of the range of operational risks and reach a level of consistency in the analysis of these risks, regardless of the method adopted, so as to establish requirements as regards the institution's funds for operational risk.

It is important to highlight that, for about ten years, the measurement space of Operational Risk evolved under the regulatory framework on risk and capital. A summary of the Basel Accords over this period of time (Basel II–Basel III) can be provided as follows: (a) to ensure that capital allocation is more risk sensitive; (b) to enhance disclosure requirements which would allow market participants to assess the capital adequacy of an institution; (c) to ensure that credit risk,

operational risk and market risk are quantified on the basis of data and formal techniques; and (d) to attempt a closer alignment of economic and regulatory capital so as to reduce the scope for regulatory arbitrage. Nowadays, the Supervisory approach has broadened the evaluation approach to procedures, tools, control system and data collection on which Operational Risk Management is based.

In fact, the Supervisory Authority, within the new SREP, analyses the operational risk along two guiding principles:

- Operational Risk Assessment;
- Operational Risk Management Assessment;

with the aim to assess not only the moment in which the capital requirement is determined, but also the procedural, organizational and managerial aspects that characterize the whole Operational Risk Management process. In the light of this, it seems that, as mentioned, even the Supervisor's view is inspired by a logic of integration of the different moments of measurement, management, control of operational losses but also integration of these different moments within the bank's business model, in the capital planning process, in the ICAAP process (*Internal Capital Adequacy Assessment Process*), the RAF (*Risk Appetite Framework*) and the bank's recovery plan. Only if the institution will be able to adopt this integrated view also for operational risk, will it be able to avoid the duplication of activities, functions, reports, information flows and, therefore, an increase of operational costs in a historical moment in which, as known, operational margins have been decreasing drastically.

Operational Risk Assessment comprises two steps, described more in detail in this section: (a) preliminary assessment; (b) assessment of the nature and significance of the institution's operational risk exposures (Fig. 2.9).

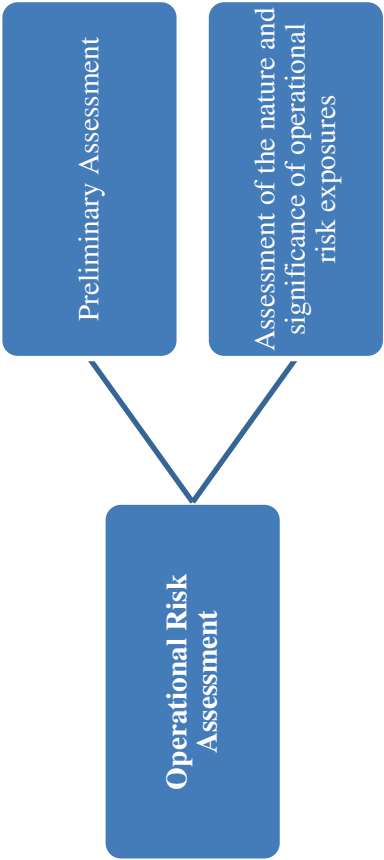


Fig. 2.9 Operational risk assessment in the new SREP. Source Author's elaboration

2.9.1 Preliminary Assessment

In the **preliminary assessment** (Fig. 2.9), competent Authorities should first identify the sources of operational risk to which the institution is exposed. To do so, they should also leverage the knowledge gained from the assessment of other SREP elements, from the comparison of the institution's position to peers (including relevant external data, where available) and from any other supervisory activities.

In this perspective, competent Authorities should consider:

- a. the main strategy for operational risk and operational risk tolerance;
- b. the business and external environments (including geographical location) in which the institution operates;
- c. the institution's own funds requirement for operational risk (distinguished by the Basic Indicator Approach (BIA), the Standardized Approach (TSA) and the Advanced Measurement Approaches (AMA)) compared to its total funds requirement and—where relevant—the internal capital for operational risk compared to the total internal capital, including the historical trends and forecasts, if available;
- d. the level of and change in gross income, assets and operational risk losses over the past few years;
- e. recent significant corporate events (such as mergers, acquisitions, disposals and restructuring), which might determine a change in the institution's operational risk profile in the short or medium term to long term (e.g. because systems, processes and procedures would not be fully aligned with the risk management policies of the parent company in the short term);
- f. changes to significant elements of the IT systems and/or of processes that might determine a change in the operational risk profile (e.g. because a new or changed IT system has not been properly tested, or because insufficient training on the new systems/processes and procedures might lead to errors);
- g. failures to comply with applicable legislation or with internal regulations as reported by external auditors and the internal audit function or brought to light by public information (bearing in mind

- both the current situation and changes in regulatory compliance behaviour over time);
- h. the ambitiousness of business plans and aggressive incentives and compensation schemes (e.g. in terms of sales targets and head-count reduction), which might increase the risk of non-compliance, human error and employee malpractice;
 - i. the complexity of processes and procedures, products (sold to customers or dealt in) and IT systems (including the use of new technologies), to the extent that they might lead to errors, delays, misspecification, security breaches, etc.; and
 - j. the institution's practices for monitoring the quality of outsourced services and its level of awareness of operational risk related to outsourced activities and of service providers' overall risk exposure pursuant to the requirements of the CEBS Guidelines on outsourcing.¹⁹

At the same time, the competent Authorities assess **the nature and significance of operational risk exposure** (i.e. the second aspect, see Fig. 2.9). Firstly, they should determine the nature of operational risk exposures and distinguish those that are more likely to lead to 'high-frequency/low-impact' events from those causing 'low-frequency/high-severity' losses (which are more dangerous from a prudential point of view) analysing exposures to the main drivers of operational risk to form a forward-looking view on potential risk and losses. This analysis may require consideration of business lines, products, processes and geographies relevant to the institution, as well as an assessment of operational risk exposures to primary risk drivers (e.g. processes, people, systems and external factors), with the use of the institution's self-risk assessment and peer analysis. In particular, competent Authorities should assess operational risk across operational risk subcategories (defined by event types and further breakdowns of these event types) and the risk drivers associated with each.

In the assessment, competent Authorities should pay particular attention to some subcategories of operational risk because of their pervasive nature and their relevance to the majority of institutions and also because of their potential prudential impact. Such subcategories include:

- a. **Conduct risk:** Since this risk covers a wide range of issues and may arise from many business processes and products, competent Authorities should leverage the outcome of the BMA and scrutinize incentive policies to gain a high-level insight into sources of conduct risk. Possible indicators of conduct risk are sanctions applied by relevant Authorities to the institution for misconduct practices; sanctions applied to peers for misconduct practices; and complaints against the institution in terms of numbers and amounts at stake.
- b. **Systems—ICT risk:** Competent Authorities may evaluate operational risk using various methodologies based on well-established industry standards [e.g. ISO 27000, Control Objectives for Information and Related Technology (COBIT) and Information Technology Infrastructure Library (ITIL)]. Competent Authorities should also assess the complexity of the IT architecture and whether it might affect the items listed above. In assessing these elements, a competent Authority should gather, where available, relevant internal incident reports and internal audit reports, as well as other indicators defined and used by the institution to measure and monitor the ICT risk.
- c. **Model risk:** Competent Authorities should assess the institution's exposure to model risk arising from the use of internal models in the main business areas and operations, following the definition and requirements specified in the Commission Delegated Regulation issued in accordance with Article 312(4) of Regulation (EU) No 575/2013 as far as they are applicable. In conducting this assessment, competent Authorities may look at the following areas, where institutions commonly make extensive use of models:
 - (a) trading in financial instruments; (b) risk measurement and management; and (c) capital allocation (including lending policies and product pricing) (Fig. 2.10).

Secondly, competent Authorities should consider the *Significance of Operational Risk* exposure. In assessing the significance of operational risk exposures, competent Authorities should consider both the

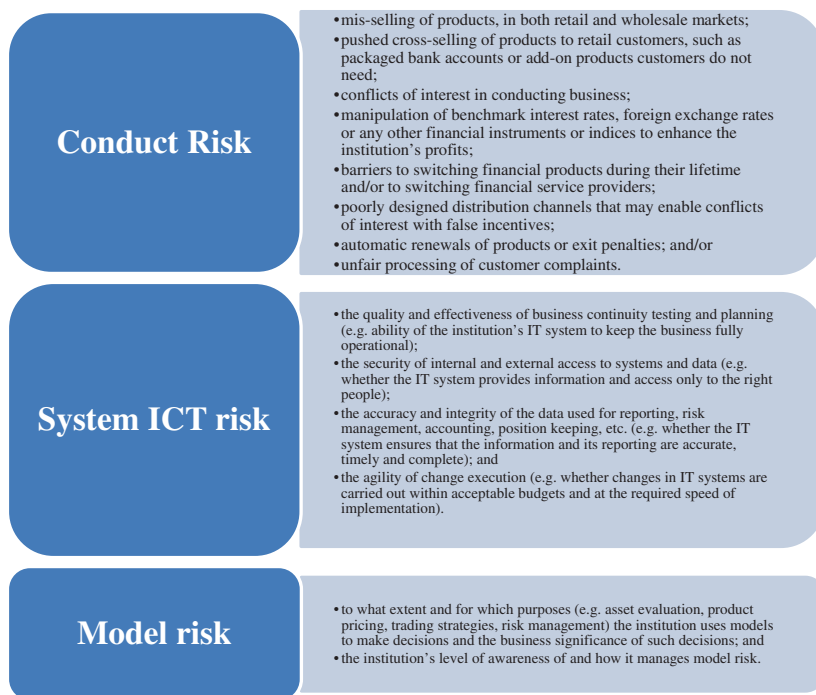


Fig. 2.10 Items considered by competent Authorities. *Source* EBA (2014)

frequency and the severity of the events to which the institution is exposed. A primary source of information that competent Authorities should consider is the institution's operational losses and event database, which, where available and reliable (i.e. accurate and complete), provides the institution's historical operational risk profile. For institutions adopting AMA, the competent Authority should also consider the output of the internal approach and also qualitative analysis. Moreover, it should leverage the institution's risk assessment, peer analysis data and public and/or consortium databases, if available and relevant (competent Authorities may consider other factors, specific to the relevant business units, etc., affected by the potential deficiencies, which can provide a measure of the risk exposure).

2.9.2 The Assessment of Operational Risk

As highlighted hereafter, in the new SREP, after the preliminary assessment, there is the Assessment of Operational Risk Management. It seems to be expired and integrated into a supervisory and evaluation approach as emphasized below. In fact, competent Authorities should assess the framework and arrangements that the institution has to specifically manage and control the operational risk as an individual risk category. This assessment should take into account:

- *the Operational Risk Management strategy and tolerance.* For this assessment, competent Authorities should take into account whether:
 - the management body clearly expresses the Operational Risk Management strategy and tolerance level, as well as the review process;
 - the senior management properly implements and monitors the Operational Risk Management strategy approved by the management body, ensuring that the institution's operational risk mitigation measures are consistent with the strategy established.
- *the organizational framework.* Competent Authorities should assess the soundness and effectiveness of the organizational framework with respect to the management of operational risk and should determine whether:
 - there are clear lines of responsibility for the identification, analysis, assessment, mitigation, monitoring and reporting of operational risk;
 - the operational risk control and monitoring systems are subject to independent review, and there is a clear separation between risk takers and risk managers, between these and the risk control and oversight risk functions;
 - the risk management, measurement and control functions cover operational risk across the entire institution (including branches) in an integrated manner, irrespective of the measurement approach

- adopted to determine the institution's minimum funds, and also cover outsourced business functions and other activities; and
- the Operational Risk Management framework is structured with sufficient and qualitatively appropriate human and technical resources.
 - *policies and procedures.* Competent Authorities should assess whether the institution has appropriate policies and procedures for the management of operational risk, including residual risk after mitigation techniques have been applied. In particular, they assess whether:
 - the management body approves the policies for managing operational risk and reviews them regularly, in line with the Operational Risk Management strategies;
 - the senior management is responsible for developing and implementing the policies and procedures for managing operational risk;
 - the Operational Risk Management policies and procedures are clearly formalized and communicated throughout the institution and cover the whole organization or at least those processes and businesses most exposed to operational risk;
 - such policies and procedures cover all the elements of Operational Risk Management, measurement and control including, where relevant, loss data collection, quantification methodologies, mitigation techniques (e.g. insurance policies), causal analysis techniques in respect of operational risk events, limits and tolerances and the handling of exceptions to those limits and tolerances;
 - the institution has implemented a new approval process for products, processes and systems that requires the assessment and mitigation of potential operational risks;
 - such policies are adequate for the nature and complexity of the institution's activities and enable a clear understanding of the operational risk inherent in the different products and activities under the scope of the institution;
 - such policies are clearly formalized, communicated and applied consistently across the institution, and for banking groups,

- whether these policies are applied consistently across the group and allow the proper management of the risk; and
- the institution promotes an Operational Risk Management culture throughout the organization, by means of training and by setting targets for operational loss reduction.
- *operational risk identification, measurement, monitoring and reporting.* Competent Authorities should assess whether the institution has an appropriate framework for Operational Risk Management in line with the institution's size and complexity and whether the framework is compliant with the regulatory framework.
 - *business resilience and continuity plans.* Competent Authorities should assess whether the institution has comprehensive and tested business resilience and continuity plans, commensurate with the nature, size and complexity of its operations in place to ensure that it is able to operate on an ongoing basis and limit losses in case of business disruption. Competent Authorities should assess the quality and effectiveness of the institution's continuity management planning process and if it includes Business Impact Analysis; appropriate recovery strategies incorporating internal and external dependencies and clearly defined recovery priorities; the drafting of comprehensive and flexible plans to deal with plausible scenarios; effective testing of the plans; and communications and crisis-management documentation and training.
 - *the internal control framework as it applies to the management of operational risk.* Competent Authorities should assess whether the institution has a strong control framework and sound safeguards to mitigate its operational risk, in line with its Operational Risk Management tolerance and strategy. Competent Authorities should also assess the functionality of the internal audit function (if it covers the main elements of Operational Risk Management measurement and control, it is effective in determining adherence to internal policies, etc.).

After the above-mentioned assessment, competent Authorities should form a view on the institution's operational risk framework. This view should be reflected in a summary of findings, accompanied by a score based on the considerations specified in Table 2.5.

Table 2.5 Supervisory considerations for assigning an operational risk score.
Source Authors' elaboration on EBA (2014)

Risk Score	Supervisory view	Consideration of inerehent risk	Consideration for adequate management & controls
1	There is no discernible risk of significant prudential impact on the institution considering the level of inherent risk and the management and controls	<ul style="list-style-type: none"> • The nature of the institution's operational risk exposure is limited to few high frequency/low-severity impact categories • The significance of the institution's exposure to operational risk is not material, as shown by scenario analysis and compared to the losses of peers • The level of losses experienced by the institution in recent years has not been material, or has decreased from a higher level 	<ul style="list-style-type: none"> • There is no discernible risk of significant prudential impact on the institution considering the level of inherent risk and the management and controls • The nature of the institution's operational risk exposure is limited to few high frequency/low-severity impact categories • The significance of the institution's exposure to operational risk is not material, as shown by scenario analysis and compared to the losses of peers • The level of losses experienced by the institution in recent years has not been material, or has decreased from a higher level
2	There is a low risk of significant prudential impact on the institution considering the level of inherent risk and the management and controls	<ul style="list-style-type: none"> • The nature of the institution's operational risk exposure is mainly high-frequency/low severity impact categories • The significance of the institution's exposure to operational risk is low, as shown by scenario analysis and compared to the losses of peers • The level of losses experienced by the institution in recent years has been low, or is expected to increase from a lower historic level or decrease from a higher historic level 	<ul style="list-style-type: none"> • There is consistency between the institution's operational risk policy and strategy and its overall strategy and risk appetite • The organizational framework for operational risk is robust with clear responsibilities and a clear separation of tasks between risk takers and management and control functions
3	There is a medium risk of significant prudential impact on the institution considering the level of inherent risk and the management and controls	<ul style="list-style-type: none"> • The nature of the institution's operational risk exposure extends to some low frequency/high-severity impact categories • The significance of the institution's exposure to operational risk is medium, as shown by scenario analysis and compared to the losses of peers • The level of losses experienced by the institution over the last few years has been medium, or is expected to increase from a lower historic level or decrease from a higher historic level 	<ul style="list-style-type: none"> • Operational risk measurement, monitoring and reporting systems are appropriate • The control framework for operational risk is sound
4	There is a high risk of significant prudential impact on the institution considering the level of inherent risk and the management and controls	<ul style="list-style-type: none"> • The nature of the institution's operational risk exposure extends to all main categories. • The significance of the institution's exposure to operational risk is high and increasing, as shown by scenario analysis and compared to the losses of peers • The level of losses experienced by the institution over the last few years has been high or risk has significantly increased 	

2.10 Some Conclusions

Operational risk measurement process is a complex system but not the most important of an Operational Risk Management infrastructure; it's only a crucial moment of this process. Authorities have been emphasizing, in this last year, the relevance of this ORM by issuing an enormous amount of guidelines and sound practices.

The need to structure an *Operational Risk Management Process* not only with reference to intermediaries that use internal models, but also to those that, although using alternative regulatory methods, produce/undergo relevant operational losses due to their business model. For those intermediaries, the lack of an *advanced measurement method* can be certainly counterbalanced by a process devoted to operational risks, proportioned to the complexity and size of the business model, capable of defining roles and responsibilities of the business units involved in the process of operational loss management. They can also develop a control and reporting system devoted expressly to operational risks and structures, and a data collection process of internal and external losses, idiosyncratic and systematic, useful for a future development of internal measurement models. In this view, it is a process that follows an integrated logic, starting from a solid management culture of Operational Risk Management, a correct definition of operational risk governance.

The great number of BCBS' guidelines and principles on *Operational Risk Management Process* allow bank to look across the enterprise in an integrated manner rather than fragmented activities to deal with a wide variety of operational risk categories.

Notes

1. The most diffused methodologies for collecting loss data in the bank system are:
 - Event driven: the 'managerial' loss datum is identified directly where the prejudicial event originated. Therefore, the datum is 'reported' directly by the decentralized organizational structures in which the loss was generated; it allows the prompt identification

of the ‘presumed’ loss events; it fosters the ‘completeness’ of the description of the event; it assumes an attention of the local structures to the themes related to operational risks; it rises the company culture; and fosters a ‘managerial’ development of operational risks through an easier identification of related prevention and/or mitigation interventions. The central structures mainly play a coordination and validation role in the collection process;

- Accounting driven: the datum is ‘extracted’ directly from the accounts; it guarantees the identification of ‘sure’ events and not assumed; it requires the existence of an analytical accounting system ‘structured’ in a consistent way with the classification present in the database of the operational losses and an enhancement of descriptive information of the event. It considers only the operational losses entered, not keeping into account events occurred but not yet entered.
2. A relevant Italian initiative consists in the observatory of the Italian Database of Operational Losses (Database Italiano delle Perdite Operative), known as Osservatorio Dipo, a non-recognized association involved in supporting the development of Operational Risk Management. The Osservatorio Dipo was launched within ABI in 2003, as an activity aimed at creating a methodology for collecting and exchanging information on operational losses incurred by the adherents. Currently, it counts about 35 members between banks and bank groups, for a total of almost 200 reporting institutions. Initiatives similar to DIPO have been launched by European associations, in which moreover several adherents to DIPO participate: among these, the *Operational Risk data and Xchange Association* (ORX, established in 2002) and the *Global Operational Loss Database* (GOLD, promoted in 2000 by the *British Bankers’ Association*). Consortia databases are being created even in the insurance field: one for all, the *Operational Risk Insurance Consortium* (ORIC), established in 2005 upon the initiative of the *Association of British Insurers*.
 3. Gareth W. Peters, Pavel V. Shevchenko, Bertrand Hassani, and Chapelle A. (2016). *Standardized Measurement Approach for Operational risk: Pros and Cons*, 3 June. <https://poseidon01.ssrn.com/delivery.php?ID=8761270200830710191260241180870310980320320050760350710680991220221040271090980741230380340630300560480391130950851030050841200190160430420410960130040190641001140930930370>

[91116003100006065010125014085117089117124075080001127019117125081098098101000116&EXT=pdf](https://www.researchgate.net/publication/31116003100006065010125014085117089117124075080001127019117125081098098101000116&EXT=pdf).

4. Cavallo, A. (2012). *Treatment of the Data Collection Threshold in Operational Risk: A Case Study with the Lognormal Distribution*, ResearchGate, p. 6.
5. It is a framework of reference which must indicate risk capacity, risk tolerance, risk appetite and early warning limits related to quantifiable risks as well as the management process of each risk.
6. It is possible to use other distributions as well, such as the binomial or negative binomial. A causal variable X has a Poisson distribution with parameter λ and is indicated with $X \sim \text{Then}(\lambda)$, if

$$P(X = n) = e^{-\lambda} \frac{\lambda^n}{n!}, \forall n \in \mathbb{N}.$$

7. It is possible to use other distributions for the body of the severity, for example the Weibull distribution. A log-normal distribution refers to a casual variable X whose logarithm follows a normal distribution. The value expected and the variance of a similar distribution are approximate to the natural logarithm of the expected value and of the variance of the normal distribution from which the log-normal originates.
8. A. Cavallo. (2012). *Treatment of the Data Collection Threshold in Operational Risk: A Case Study with the Lognormal Distribution*, ResearchGate, p. 5.
9. S. Borra A. Di Ciaccio (2008). *STATISTICA metodologie per le scienze economiche e sociali*, McGraw-Hill, p. 309.
10. The Peaks Over Threshold method allows to consider values that the causal variable X assumes beyond the threshold u . These extreme values, called also excesses, are described through the conditioned probabilities.
11. The correlation matrix is calculated with the Tau of Kendall method or the Rho of Spearman method.
12. Sklar's Theorem: each joint distribution can be written as a copula function that has marginal distributions as topics; any copula function that has distributions as topics is a joint distribution.
13. Jarow Robert A. (2006). *Operational risk*. www.researchgate.net/profile/Robert_Jarow/publication/222530698_Operational_Risk/links/0046352384826ac93e000000.pdf.

14. BCBS. (2006). *International Convergence of Capital Measurement and Capital Standards: a Revised Framework*. Comprehensive Version, Basel Committee on Banking Supervision, p. 144. <http://www.bis.org/publ/bcbs128.htm>.
15. BCBS. (2011). *Principles for the Sound Management of Operational Risk*. Basel Committee on Banking Supervision, pp. 13–14. www.bis.org/publ/bcbs195.htm.
16. Ibid.
17. EBA. (2014). *Guidelines on Common Procedures and Methodologies for the Supervisory Review and Evaluation Process (SREP)*. [www.eba.europa.eu/documents/10180/1051392/EBA-GL-2014-13+GL+on+Pillar+2+\(SREP\)%20-IT.pdf/03cdf635-2f85-41f0-b078-1da40d63ef64](http://www.eba.europa.eu/documents/10180/1051392/EBA-GL-2014-13+GL+on+Pillar+2+(SREP)%20-IT.pdf/03cdf635-2f85-41f0-b078-1da40d63ef64).
18. Ibid., p. 93.
19. Ibid., p. 95.

References

- Bank of Italy. (2013). Circolare 285/2013. Disposizioni di vigilanza per le banche. www.bancaditalia.it/compiti/vigilanza/normativa/archivio-norme/circolari/c285/index.html.
- BCBS. (1998). *Operational Risk Management*. Basel Committee on Banking Supervision. <http://www.bis.org/publ/bcbs42.pdf>.
- BCBS. (2001a). *Operational Risk. Supporting Document to the New Basel Capital Accord*. Basel Committee on Banking Supervision, Consultative Document. www.bis.org/publ/bcbsca07.pdf.
- BCBS. (2001b). *The Internal Ratings-Based Approach*. Basel Committee on Banking Supervision, Consultative Document. www.bis.org/publ/bcbsca05.pdf.
- BCBS. (2004). *International Convergence of Capital Measurement and Capital Standards*. Basel Committee on Banking Supervision. <http://www.bis.org/publ/bcbs107.htm>.
- BCBS. (2006). *International Convergence of Capital Measurement and Capital Standards: A Revised Framework*. Comprehensive Version, Basel Committee on Banking Supervision. <http://www.bis.org/publ/bcbs128.htm>.

- BCBS. (2009a). *Observed Range of Practice in Key Elements of Advanced Measurement Approaches (AMA)*. Basel Committee on Banking Supervision. <http://www.bis.org/publ/bcbs160b.pdf>.
- BCBS. (2009b). *Results from the 2008 Loss Data Collection Exercise for Operational Risk*. Basel Committee on Banking Supervision. www.bis.org/publ/bcbs160a.pdf.
- BCBS. (2011a). *Operational Risk—Supervisory Guidelines for the Advanced Measurement Approaches*. Basel Committee on Banking Supervision. www.bis.org/publ/bcbs196.htm.
- BCBS. (2011b). *Principles for the Sound Management of Operational Risk*. Basel Committee on Banking Supervision. www.bis.org/publ/bcbs195.htm.
- BCBS. (2014). *Operational Risk—Revisions to the Simpler Approaches*. Basel Committee on Banking Supervision, Consultative Document. <http://www.bis.org/publ/bcbs291.pdf>.
- BCBS. (2016). *Standardised Measurement Approach for operational Risk*. Basel Committee on Banking Supervision, Consultative Document, March. <http://www.bis.org/bcbs/publ/d355.pdf>.
- Bee, M. (2005). On Maximum Likelihood Estimation of Operational Loss Distributions. *University of Trento Department of Economics Working Paper*, (2005-03).
- Birindelli, G., & Ferretti, P. (2009). Il rischio operativo nelle banche italiane. Modelli, gestione e disclosure. Bancaria editrice.
- Birindelli, G., & Ferretti, P. (2017). *Operational Risk Management in Banks*. Palgrave Macmillan.
- Borra, S., & Di Ciaccio, A. (2008). *Statistica. Metodologie per le scienze economiche e sociali*. McGraw-Hill.
- Cavallo, A., Rosenthal, B., Wang, X., & Yan, J. (2012). Treatment of the data collection threshold in operational risk: A case study with the lognormal distribution. *The Journal of Operational Risk*, 7(1), pp. 3–38.
- Chapelle. (2013). The Importance Preventive KRIs. *Operational Risk & Regulation*, No. 58.
- Cope, E. W., Mignola, G., Antonini, G., & Ugoccioni, R. (2009). Challenges and pitfalls in measuring operational risk from loss data. *The Journal of Operational Risk*, 4(4), No. 3, pp. 3–38.
- Cornalba, C., & Giudici, P. (2004). Statistical models for operational risk management. *Physica A: Statistical Mechanics and its Applications*, 338(1), pp. 166–172.

- Cosma, S. (2006). La misurazione del rischio operativo nelle banche: Basilea 2, regole nazionali ed europee, approcci, modelli e tecniche innovativi. Bancaria editrice.
- Cosma, S., Dell'Anna, L., & Salvadori, G. (2014). Dal Risk Self Assessment alla stima del Value-at-Risk operativo: una proposta metodologica. *Bancaria*, No. 11.
- Cruz, M. G. (2002). *Modeling, Measuring and Hedging Operational Risk*. Wiley-Finance.
- Cruz, M. G. (2004). *Operational Risk Modelling and Analysis: Theory and Practice*. London: Risk Books.
- Cruz, M., Peters, G., & Shevchenko, P. (2015). *Fundamental Aspects of Operational Risk and Insurance Analytics: A Handbook of Operational Risk*. USA: Wiley-Finance.
- De Polis, S. (2015). L'approccio di vigilanza alla funzione organizzazione nelle banche: tra business ed esigenze di governo. L'uscita dall'eclissi parziale. Banca d'Italia. www.bancaditalia.it/pubblicazioni/interventi-vari/int-var-2015/depolis-020715.pdf.
- EBA. (2014). *Guidelines on Common Procedures and Methodologies for the Supervisory Review and Evaluation Process*. European Banking Authority. www.eba.europa.eu/-/eba-publishes-final-guidelines-on-srep-methodologies-and-processes.
- EBA. (2015). *RTS on AMA Assessment*. European Banking Authority. www.eba.europa.eu/documents/10180/1100516/EBA-RTS-2015-02+RTS+on+AMA+assessment.pdf.
- EBA. (2016). *Guidelines on ICAAP and ILAAP Information Collected for SREP Purposes*. European Banking Authority. www.eba.europa.eu/-/eba-publishes-final-guidelines-on-icaap-and-ilaap-information.
- ECB. (2016). *SSM SREP Methodology Booklet*. European Central Bank. www.bankingsupervision.europa.eu/ecb/pub/pdf/ssm_srep_methodology_booklet.en.pdf.
- Embrechts, P., & Puccetti, G. (2008). Aggregating risk across matrix structured loss data: The case of operational risk. *Journal of Operational Risk*, 3(2), pp. 29–44.
- Embrechts, P., Furrer, H., & Kaufmann, R. (2003). Quantifying regulatory capital for operational risk. *Derivatives Use, Trading and Regulation*, 9(3), pp. 217–233.
- European Parliament and Council. (2013). Directive 2013/36/EU on access to the activity of credit institutions and the prudential supervision of credit

- institutions and investment firms, amending Directive 2002/87/EC. <http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32013L0036&from=IT>.
- European Parliament and Council. (2013). Regulation (EU) No 575/2013 on prudential requirements for credit institutions and investment firms and amending Regulation (EU) No 648/2012. <http://eur-lex.europa.eu/legal-content/IT/TXT/?uri=celex%3A32013R0575>.
- Figini, S., Gao, L., & Giudici, P. (2013). *Bayesian operational risk models*. Department of Economics and Management, University of Pavia, 47.
- Franzetti, C. (2016). *Operational Risk Modelling and Management*. CRC Press Book.
- Girling, P. X. (2013). *Operational Risk Management: A Complete Guide to a Successful Operational Risk Framework*. USA: Wiley-Finance.
- Giudici, P. (2004). Integration of qualitative and quantitative operational risk data: A Bayesian approach. *Operational Risk Modelling and Analysis, Theory and Practice* (pp. 131–138). London: RISK Books.
- Guegan, D., & Hassani, B. K. (2013). Operational risk: A Basel II step before Basel III. *Journal of Risk Management in Financial Institutions*, 6(1), pp. 37–53.
- Gustafsson, J., & Nielsen, J. P. (2008). A mixing model for operational risk. *Journal of Operational Risk*, 3(3), pp. 25–38.
- Hillson, D. A., & Hulett, D. T. (2004). Assessing risk probability: Alternative approaches. *PMI Global Congress Proceeding* (pp. 1–5). Czech Republic, Prague.
- Ieva, F., Paganoni, A. M., & Ziller, S. (2013). Operational risk management: A statistical perspective. *Far East Journal of Mathematical Sciences*, No. 23.
- Jarrow, R. A. (2008). Operational risk. *Journal of Banking & Finance*, 32(5), pp. 870–879.
- Jobst, A. (2007). *Operational Risk: The Sting is Still in the Tail But the Poison Depends on the Dose*. International Monetary Fund, pp. 7–239.
- King, J. L. (2001). *Operational Risk: Measurements and Modelling*. USA: Wiley.
- Lamanda, G. (2011). *Regulation and practice of managing the banks operational risks*. Ph.D. thesis, Budapest University of Technology and Economics.
- Lamanda, G., & Vöneki, Z. T. (2015). Hungry for risk. A risk appetite framework for operational risks. *Public Finance Quarterly*, 60(2), pp. 212–225.
- Leadbetter, M. R. (1991). On a basis for peaks over threshold modeling. *Statistics & Probability Letters*, 12(4), pp. 357–362.

- Lopez, J. A. (2002). What is operational risk. *FRBSF Economic Letter*, 2, pp. 1–4.
- Moosa, I. A. (2007a). Operational risk: A survey. *Financial Markets, Institutions & Instruments*, 16(4), pp. 167–200.
- Moosa, I. A. (2007b). Misconceptions about operational risk. *Journal of Operational Risk* 1 (Winter), pp. 97–104.
- Moosa, I. A. (2007c). *Operational Risk Management*. London: Palgrave.
- Moosa, I. A. (2007d). *A Critique of the Advanced Measurement Approach to Regulatory Capital Against Operational Risk* (Working paper). Monash University.
- Moscadelli, M. (2004). *The modelling of operational risk: Experience with the analysis of the data collected by the Basel Committee*. Bank of Italy, Economic Research and International Relations Area, No. 517.
- Neil, M., Häger, D., & Andersen, L. B. (2009). Modeling operational risk in financial institutions using hybrid dynamic Bayesian networks. *The Journal of Operational Risk*, 4(1), No. 3.
- Peters, G. W., Shevchenko, P. V., Hassani, B. K., & Chapelle, A. (2016). *Standardized Measurement Approach for Operational risk: Pros and Cons*. Université Panthéon-Sorbonne (Paris 1), Centre d'Economie de la Sorbonne, No. 16064.
- Robertson, D. (2016). *Managing Operational Risk: Practical Strategies to Identify and Mitigate Operational Risk Within Financial Institutions*. London, UK: Palgrave Macmillan.
- Rozenfeld, I. (2010). *Using shifted distributions in computing operational risk capital*. Available at SSRN: <https://ssrn.com/abstract=1596268>.
- Shevchenko, P. V. (2011). *Modelling Operational Risk Using Bayesian Inference*. Springer Science & Business Media.
- Sklar, M. (1959). Fonctions de répartition à n dimensions et leurs marges. Université Paris, No. 8.
- SSG. (2009). *Risk Management Lessons from the Global Banking Crisis of 2008*. Senior Supervisors Group. www.fsb.org/2009/10/r_0910.
- Valová, I. (2011). Basel II approaches for the calculation of the regulatory capital for operational risk. Masaryk University, Faculty of Economics and Administration.
- Vinella, P., & Jin, J. (2005). A foundation for KPI and KRI. *Operational Risk: Practical Approaches to Implementation* (pp. 157–168).

Measuring and Managing Operational Risk
An Integrated Approach

Leone, P.; Porretta, P.; Vellella, M. (Eds.)

2018, XX, 211 p. 40 illus., Hardcover

ISBN: 978-3-319-69409-2