NATIONAL SECURITY
НАЦИОНАЛНА СИГУРНОСТ

QUANTIFICATION OF OPERATIONAL RISKS IN GERMAN BANKS AS AN ELEMENT OF NATIONAL SECURITY

Florian Becker
University of Library Studies and Information Technologies
https://doi.org/10.70300/UJIM4140

Abstract: *Risk management is a central pillar of modern banking, serving market-driven objectives, regulatory requirements aimed at safeguarding financial stability and national security alike. Within this framework, operational risk (OpRisk) represents one of the four major risk types alongside credit, market, and liquidity risk. This paper examines how German banks can quantify OpRisk for the purpose of economic risk-bearing capacity as an element of national security. Building on regulatory foundations such as MaRisk and the Basel framework, two key data sources are emphasized: historical loss databases and forward-looking risk assessments. Their combined use allows banks to capture both past events and potential future risks. For quantification, the loss distribution approach is applied, separating frequency and severity distributions and aggregating them through Monte Carlo simulation to derive a comprehensive loss distribution. Additional structuring into business lines and event categories enables granular modelling and the incorporation of dependencies through correlation assumptions. The study illustrates an exemplary, though widely established, methodology that provides banks with a statistically sound basis for determining Value-at-Risk at a 99.9% confidence level and integrating it into risk-bearing capacity calculations. While variations in implementation remain, the model demonstrates how quantitative methods can strengthen operational resilience and contribute to systemic stability as well as national security.*
Keywords: *operational risk; risk bearing capacity; loss distribution, risk management*

INTRODUCTION

Risk management is an integral part of business operations for banks today. However, from a bank's perspective, the motivation for risk management is not exclusively intrinsic in nature, but can be divided into two aspects. From a market-driven perspective, risk management plays a supporting role in corporate management and in achieving objectives, as mentioned above. From a regulatory and legal perspective, however, there are also requirements that serve to protect creditors and the entire financial system (Strauß 2008, p. 34). The financial system is based on financial stability, so to speak. Financial stability refers to a state in which the financial system can smoothly fulfil its core functions, e.g. lending and payment transactions. Such a system not only prevents financial crises, but is also directly linked to national security. National security strategies usually even include the resilience of the financial sector. Therefore, it can be argued that national security also depends significantly on efficient and resilient operational risk management in banks, since it also needs financial security and a resilient financial system.

The last financial crisis in 2008 clearly showed that deficits in the operational risk management of individual actors or banks are sufficient to cause insolvencies. Conversely, these insolvencies or financial difficulties can result in a chain action that, as in the past, affects the stability of the financial system. Although such crises are unlikely to repeat themselves completely identically, similar effects are also imaginable in today's world. While the financial difficulties of individual EU member states in recent years cannot be attributed exclusively to banking crises, they illustrate the potential danger that underlies the European Union's financial system. Around 2009/2010, for example, Greece was plunged into a major sovereign debt crisis. In this context, immense rescue packages from other EU member states have flowed to Greece not long afterwards. However, the situation also worsened seriously for other member states, which put Italy, Portugal and other countries in financial difficulties as well. Such a chain of circumstances is also quite conceivable with regard to the banking sector. Attempts to rescue other banks or states could also trigger a chain reaction that would exacerbate the financial problems of one or more banks rather than solve them in the long term. However, financial security has several levels that go beyond the mere stability of the financial system. Other companies associated with financial service providers may also be affected. Bank failures and insolvencies can also have a massive impact on companies that have loans. If, for example, loans are no longer available to strengthen and stabilise production and manufacturing, this may result in a crash in profits. The same applies to consumers and households. Many households depend on the stability of banks and the financial sector for real estate financing or other loans and financial products. When problems arise, their own real estate, savings and the entire financial security of private households are sometimes at risk. The combination of potential impacts on the financial sector and private households also makes it clear that the state as such is also dependent on a stable banking system. The dimensions in this context are diverse. There may be a loss of trust in the financial system. Problems in the financial system can lead to lower tax revenues and, as a result, problems for the state. Potential financial support for banks, as in the past, can also be extremely costly for the state. In summary, due to the potential far-reaching consequences, the national security of entire countries is affected by the issue.

In this context, it is the task of a bank's risk management to determine the appropriate level of capital adequacy. If institutions are not permanently able to offset losses, there is a risk of insolvency which might result in a chain reaction with effect to national security like it did during the last financial crisis. To prevent this, the legal framework for financial institutions provides for a sufficient liquidity buffer with an appropriate loss buffer in the form of equity capital. When calculating risk-bearing capacity (RBC), two approaches are distinguished. On the one hand, there is the normative perspective and, on the other, the economic perspective. The normative perspective comprises an annual review and capital planning over a planning horizon of at least three years. This planning is divided into a planned scenario (base scenario) and an adverse scenario. The perspective that is more relevant to this paper is that of economic risk-bearing capacity. In this context, present-value risks are compared with an economic risk coverage amount, which in the best case corresponds to the company's present value. The risks are usually risk indicators on a one-year risk horizon with a confidence level of at least 99.9%. Put simply, this means that all risks with a probability of occurrence greater than 0.1% must be quantitatively taken into account in the RBC. To provide a brief overview of the industry, it can be said that smaller companies on average also have weaker equity capitalisation in percentage terms. Companies with annual revenues of up to €2 million have average coverage of 18.5%, while companies with annual revenues between €25 million and €50 million already have an average ratio of 30.3%. In the range between €50 million and €250 million, the ratio is approximately 31.9% (Mohr & Rödl 2017, p. 135). Adequate equity capital is particularly important for banks because they play a key role in the stability of the financial system (Ercoc & Met & Seker 2023, p. 1000).

In the context of risk management at banks, OpRisk is often referred to as one of the main types of risk alongside counterparty default risk, market risk and liquidity risk. OpRisk has different meanings in the banking sector, and different institutions use their own definitions for internal purposes. However, it is important to note that all definitions take into account the regulatory definition of operational risk in the narrower sense. According to the Capital Requirements Regulation (CRR), OpRisk is defined as the risk of loss resulting from inadequate or failed internal processes, people, systems, or from external events, including legal risks.

This paper aims to illustrate how German banks can quantify their operational risks for the economic perspective of risk-bearing capacity to strengthen their risk management and be more resilient in view of financial stability.

RESEARCH METHODOLOGY

The basic functioning of a model for quantifying operational risks in banks is to be illustrated within the framework of a theoretical conception of such a model. The core methodology is the

Loss Distribution Approach, which originally comes from actuarial science. By modelling the frequency and severity of loss events separately and then aggregating them using Monte Carlo simulation, reliable loss distributions can be derived. On this basis, value-at-risk values can be determined up to a 99.9% confidence level and integrated into the calculation of risk-bearing capacity. The representation of the risk cell structure also illustrates how different business areas and event categories can be considered separately and potential correlations can be embedded.

The relevant technical and statistical background for this approach is derived from a literature analysis using the online database ResearchGate. In addition, the relevant regulatory requirements, in this case the Minimum Requirements for Risk Management (MaRisk) and the requirements of the Basel Framework, were analyzed.

RESULTS

In addition to MaRisk, there is also the Basel framework. These are capital adequacy requirements published by the Basel Committee on Banking Supervision, based in Basel, in December 2010 and December 2017. These requirements stipulate, for example, that banks must maintain an internal loss database and use it to quantify operational risk (Kudinska & Sobanova 2022, p. 123).

These have a modular structure and contain specific requirements for the management and control processes for individual risk types as well as for risk reporting (Müller 2022, p. 98).

In addition to regular, mandatory reporting of current risks, two key instruments for managing and quantifying risks can be distinguished in the area of operational risk: a loss database and a risk assessment.

1. Loss database

Another key component of the operational risk management is the loss database. This is a database of OpRisk losses that have already occurred. In addition to the amount of the loss and the date of occurrence, any measures taken and a description of the course of events or background to the loss are also recorded. The database is used to build up historical loss data at institutional level. Cases are usually recorded above a certain loss amount, which often ranges between €1,000 and €5,000, depending on the bank (Hartmann-Wendels et al. 2014, p. 416). In addition, it is also possible to record known risks in the database in a standardised manner. Since the internal database is often not extensive enough to perform statistical calculations based on it, internal data is often supplemented with external data pools (e.g. ORX) in practice.

The historical data also forms the basis for statistical modelling of OpRisk, which in turn is required for inclusion in the bank's RBC calculation (Hager & Romeike 2020, p. 156).

2. Risk assessment

As already mentioned, the risk management process begins with the identification of risks. This also applies to the operational risk management (Baijal 2021, p. 254). Risks are usually identified primarily through a risk assessment. This refers to the general process of risk identification, analysis and evaluation. Essentially, this is the basis and starting point for the entire process (Lyon & Popov 2017, p. 35).

Conceptually, the survey is usually conducted in the form of structured questionnaires. Although there are certain differences in detail, the questions generally cover the amount and frequency of potential losses, the quality of processes and possible measures (Maslen 2010, p. 29).

Based on these two data sources, it is possible to quantify the RBC. The combination of both data sets is particularly important because historical data can only take into account events that have already occurred and therefore does not cover potential risks that do not appear in the historical data. In order to take the individual risks of specific institutions into account appropriately, it therefore makes sense to supplement the historical data with forward-looking, possibly theoretically oriented risk queries in order to obtain as comprehensive and realistic a picture as possible for the quantification.

There are various mathematical and statistical methods that can be used to perform quantification. Historical loss data is often used to model the probabilities of occurrence and the amounts of damage separately. To obtain a distribution estimate for the frequency, Poisson, binomial or negative binomial distributions can be used, for example. For severity, on the other hand, lognormal, Pareto, Weibull or generalized Pareto distributions are commonly used. The distributions are then aggregated using a Monte Carlo simulation to obtain an overall risk distribution, i.e. the value at risk (VaR) (see Fig. 1). Since operational risks are often correlated with each other (e.g. an IT failure may lead to legal or reputational risks), there are also many copula models for mapping these dependencies using multivariate modelling and aggregation.

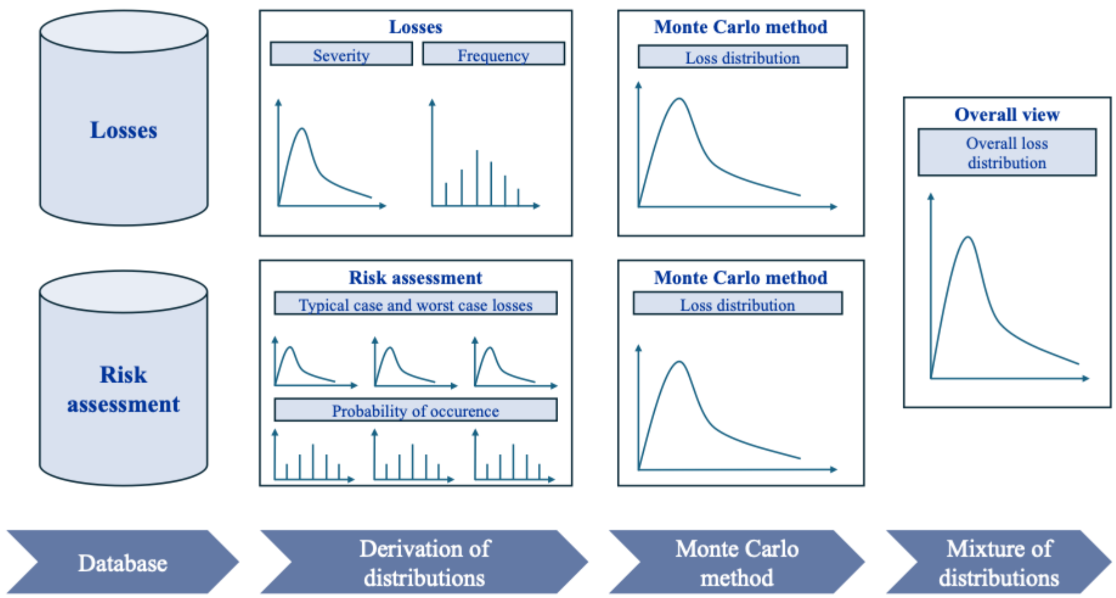

Fig. 1. Four steps of OpRisk quantification

In a sense, the quantification of operational risks can be divided into four steps. The creation of an appropriate database has already been discussed as a basic prerequisite. Building on this, two distributions with the data points contained in there are first generated from the data source of empirical claims. On the one hand, there is a distribution for the amounts of damage, which is derived from the individual damage sums, and on the other hand, there is a distribution of the frequencies of claims, which is formed from the respective occurrence data.

Similarly, two distributions are also generated from the data in the expert estimate. Technically, this works by requiring the experts to estimate the amount of average damage and extreme damage in some form. Put simply, the average damage then represents the maximum of the damage distribution, while the maximum damage limits the distribution on the abscissa to the right.

After deriving the distributions, both distributions per data source are combined into a loss distribution using a statistical method. Monte Carlo simulation is typically used for this purpose.

Random numbers are generated from the existing data in order to statistically map as many future scenarios as possible. An example of this process is as follows:

1. The number of losses in a year is drawn from the frequency distribution.
   a. Example: 7 losses.
2. For each loss, a loss amount is drawn from the severity distribution.
   a. Example: 7 losses with amounts [0.5 million; 2 million; 0.3 million; ...].
3. All losses are added together to give a total annual loss.
   a. Example: EUR 9.1 million.

This process is repeated thousands or even millions of times, so that ultimately a statistically usable empirical loss distribution function can be derived from it.

In the fourth and final step, the overall view, i.e. the combination of the annual losses from both Monte Carlo simulations, is converted into a combined loss distribution. The 99.9% quantile value of this distribution represents the VaR required by the supervisory authorities for the RBC.

Certain dependencies between different categories of operational risk can be modelled by dividing the input data into specific categories in advance. In collaboration with the banking sector, the Basel Committee has defined the following seven event types that encompass OpRisk. These categories are intended to cover aspects of banking operations that can result in large operational losses. The first level of categories can be further broken down into a specific second level and a third level with explicit examples (Maslen 2010, p. 11). In addition to these seven categories, the business areas defined in accordance with CRR are also suitable for this purpose (see Fig. 2).

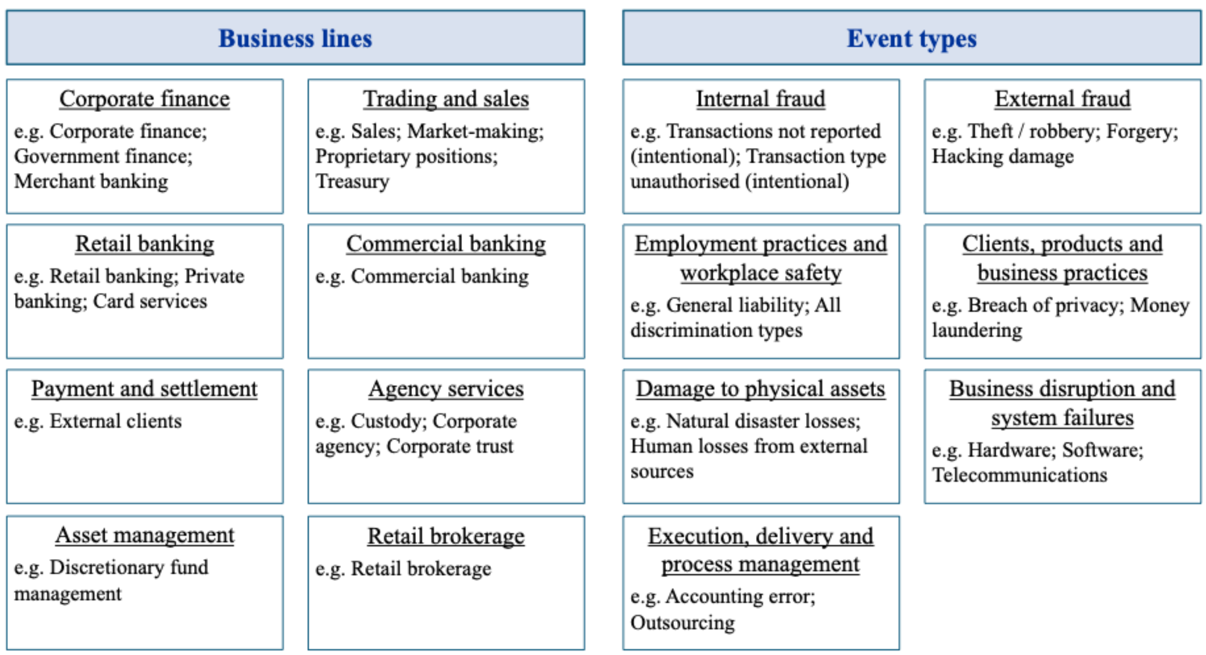

Fig. 2. Overview of business lines and event types according to the CRR

Before quantification can begin, all input data must first be assigned to the corresponding business areas and event categories. This also involves a corresponding dependency on external data, as this should ideally have identical mapping to the internal loss data for consistency reasons. The risk assessment must also be structured in advance in such a way that all data points and values can be assigned to a business area and an event category without overlap.

If the input data is parameterized accordingly, the model can also be constructed in a matrix structure of 'risk cells', each combining a business area and an event category, i.e. a total of 56 risk cells (see Fig. 3).

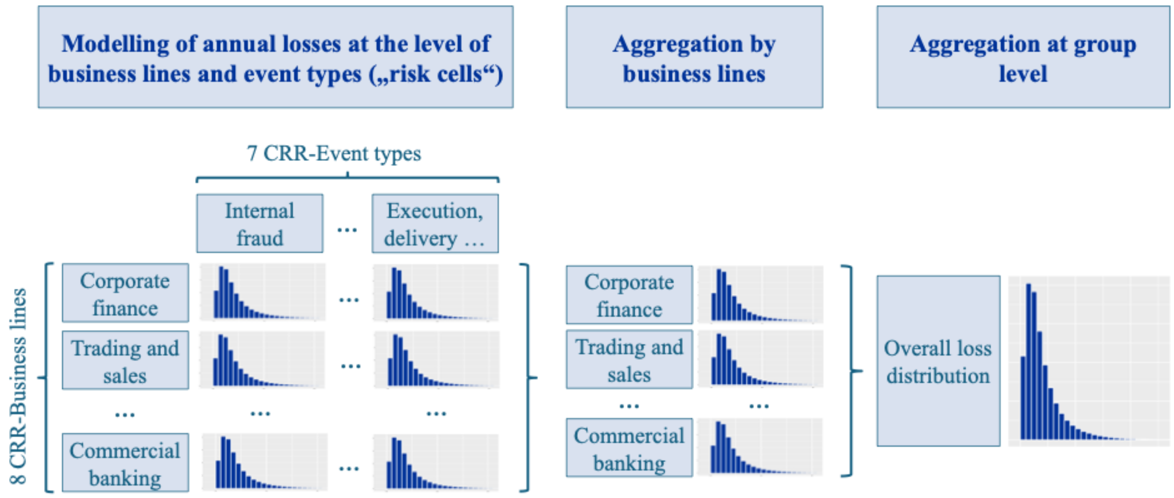

Fig. 3. Exemplary matrix structure of an OpRisk model

The methodology differs only slightly from the example procedure described above; in fact, the statistical methods are completely identical. The various functions are simply formed at a granular level. In the first step, a function for annual losses is formed for each risk cell (e.g. internal fraud & corporate finance) from all assigned data sets. As described above, this results from the combination of the two distributions for the amount and frequency of loss events.

In the second step, after a distribution has been generated for each of the 56 risk cells, these are aggregated at a higher level. It does not matter whether the distributions are aggregated at the business area level or at the event category level. In the example shown here, the aggregation is performed at the business area level, resulting in eight distributions for annual losses. In the final step, these eight functions are combined to form an overall group loss distribution, from which the VaR can then be derived.

Compared to the simplified version, this methodology has the advantage that any correlations between different business areas and event categories can be mathematically represented by assuming certain predefined correlation assumptions when aggregating the distributions from the business area level and at the group level, and integrating them into the model. The distributions are therefore not superimposed 1:1, but it is assumed that certain risks or losses occur more frequently together, or that when certain risks or losses occur, other circumstances cannot occur, which influences the aggregated function accordingly.

The calculation concept is also known as the loss distribution approach and originally comes from the field of actuarial science. Mathematically, this can be expressed as follows:

$$S = \sum_{k=1}^{N} X_k$$

Here, „N“ is the random number of loss events, while „X_k“ represents the random amount of each individual loss.

„N“ describes the number of claims per year in the value range [0, 1, 2, 3, ...] and is typically modelled using a Poisson distribution. Assuming that the distribution is independent of the amount of damage, this gives the expected number of loss events within a year.

„X_k“ describes the amount of the k’th loss in a year in a value range [0, ¥]. The variable is modelled by a right-skewed distribution, which means that there are a large number of small losses with low amounts and a few serious large losses. The assumption here is that all losses originate from the same distribution and that individual losses are independent of each other.

„$k = 1$“ refers to the summation index in the formula and marks the starting value of the count. This means that the summation begins with the first loss event.

CONCLUSION

This paper has shown how German banks can quantify their operational risks within the framework of economic risk-bearing capacity. The starting point for this is both regulatory requirements – in particular MaRisk and Basel regulations – and economic requirements for adequate capitalization. An important aspect, regardless of the point of view, is the strengthening of resilience and thus national security. A key component is the use of two data sources: on the one hand, historical losses, which are systematically recorded in a loss database, and on the other hand, risk-oriented assessments in the form of risk assessments. Only the combination of both approaches enables the most comprehensive possible representation of the risk situation, as historical data alone cannot sufficiently take future developments into account.

It should be emphasized that the procedures described are examples of a widely used approach in practice. The specific design – such as the choice of distributions, the calibration of parameters or the assumptions about correlations – may vary depending on the institution, the data available and the regulatory environment. Nevertheless, the methodology described here illustrates the basic functioning and the essential steps of a statistically sound quantification of operational risks.

Overall, it is clear that a methodologically sound and practical model not only meets regulatory requirements but also serves as an essential tool for internal risk management. In this way, banks can strengthen their resilience to operational risks and thus make an important contribution not only to the stability of the financial system but to national security as well.

The findings of the paper are limited in that they merely represent an example of how operational risks in banks can be quantified. The reality is sometimes very diverse and requires further research in the future with regard to differences in the approaches. Current topics such as ESG, sustainability and artificial intelligence will also influence the quantification of operational risks in banks in the future and should be examined accordingly.

REFERENCES

BAIJAL, R., 2021. Identification, quantification and monitoring of operational risk. *Journal of Securities Operations & Custody*, vol. 13, no. 3, pp. 235–263.

ERKOC, A.; MET, I.; SEKER, S., 2023. Performance, efficiency and target setting for bank branches: Time series with automated machine learning. *IEEE Access*, vol. 11, pp. 1000–1010.

HAGER, P.; ROMEIKE, F., 2020. *Erfolgsfaktor Risikomanagement 4.0: Methoden, Beispiele, Checklisten – Praxishandbuch für Industrie und Handel*. Wiesbaden: Springer Gabler.

HARTMANN-WENDELS, T.; SCHLÜTER, T.; WEBER, T.; ZANDER, M., 2017. Die Risikoberichterstattung deutscher Banken: Erhebung des Branchenstandards. *Schmalenbach Journal of Business Research*, vol. 66, pp. 368–427.

KUDINSKA, M.; SOBANOVA, J., 2022. New tendencies in operational risk management in banks: Challenges and opportunities. *Humanities and Social Sciences Latvia*, vol. 30, no. 1, pp. 108–125.

LYON, B.; POPOV, G., 2017. Communicating and managing risk: The key result of risk assessment. *Professional Safety*, vol. 62, pp. 35–44.

MASLEN, M., 2008. *Steuerung und Reduktion operationeller Risiken im Bankensektor*. Hamburg: Diplomica.

MOHR, B.; RÖDL, H., 2017. Wachsendes Eigenkapital stärkt Stabilität des deutschen Unternehmenssektors. In: *Betriebswirtschaftliche Fragen zu Steuern, Finanzierung, Banken und Management*, pp. 131–143. Wiesbaden: Springer Gabler.

MÜLLER, K., 2022. *Handbuch Unternehmenssicherheit: Umfassendes Sicherheits-, Kontinuitäts- und Risikomanagement mit System*. Wiesbaden: Springer Vieweg.

STRAUSS, M., 2008. *Wertorientiertes Risikomanagement in Banken: Analyse der Wertrelevanz und Implikationen für Theorie und Praxis*. Wiesbaden: Gabler.

КОЛИЧЕСТВЕНО ИЗМЕРВАНЕ НА ОПЕРАТИВНИТЕ РИСКОВЕ В ГЕРМАНСКИТЕ БАНКИ КАТО ЕЛЕМЕНТ ОТ НАЦИОНАЛНАТА СИГУРНОСТ

Резюме: *Управлението на риска е централен стълб на съвременното банкиране, който служи на пазарно ориентирани цели и регулаторни изисквания, насочени към опазване на финансовата ста-*

билност и националната сигурност. В тази рамка оперативният риск (OpRisk) представлява един от четирите основни вида риск, наред с кредитния, пазарния и ликвидния риск. В настоящата статия се разглежда как германските банки могат количествено да измерват OpRisk с цел определяне на икономическата рискоустойчивост като елемент на националната сигурност. Въз основа на регулаторни основи като MaRisk и Базелската рамка се подчертават два ключови източника на данни: бази данни за исторически загуби и прогнозни оценки на риска. Тяхното комбинирано използване позволява на банките да отразят както минали събития, така и потенциални бъдещи рискове. За количествено измерване се прилага подходът на разпределение на загубите, като разпределенията се разделят по честота и тежест и се агрегират чрез симулация на Монте Карло, за да се получи цялостно разпределение на загубите. Допълнителното структуриране по бизнес линии и категории събития позволява детайлно моделиране и включване на зависимости чрез корелационни предположения. Проучването илюстрира примерна, макар и широко установена методология, която предоставя на банките статистически обоснована основа за определяне на стойността на риска при 99,9% ниво на достоверност и интегрирането ѝ в изчисленията на капацитета за поемане на риск. Въпреки че все още съществуват различия в прилагането, моделът показва как количествените методи могат да укрепят оперативната устойчивост и да допринесат за системната стабилност, както и за националната сигурност.

Ключови думи: *оперативен риск; капацитет за поемане на риск; разпределение на загубите; управление на риска*

Флориан Бекер, докторант
Университет по библиотекознание и информационни технологии
София, България
E-mail: flo.becker@online.de