ISSN (Print) 2307-6968, ISSN (Online) 2663-2209
Вчені записки Університету «КРОК» №2 (82), 2026

УДК 658.1 : 330.1
DOI: 10.31732/2663-2209-2026-82-253-266

Дата надходження: 17.04.2026
Дата прийняття до друку: 15.05.2026
Дата публікації: 30.05.2026

ПІДХОДИ ЩОДО ОЦІНКИ ОПЕРАЦІЙНОГО РИЗИКУ У ФІНАНСОВИХ УСТАНОВАХ

***Дмитро Коваль*[1]**

[1]Аспірант кафедри управлінських технологій, ВНЗ «Університет економіки та права «КРОК», м. Київ, Україна, e-mail: KovalDV@krok.edu.ua, ORCID: https://orcid.org/0009-0004-7314-3114

APPROACHES TO OPERATIONAL RISK ASSESSMENT IN FINANCIAL INSTITUTIONS

***Dmytro Koval*[1]**

[1]Postgraduate student, Department of Management Technologies, KROK University, Kyiv, Ukraine, e-mail: KovalDV@krok.edu.ua, ORCID: https://orcid.org/0009-0004-7314-3114

Анотація. *У статті досліджено підходи до оцінки операційного ризику у фінансових установах з акцентом на кількісні, якісні та змішані методи в умовах зростання невизначеності, спричиненої воєнними, геополітичними, технологічними та регуляторними чинниками. Розглянуто теоретичні основи традиційних метрик (добуток імовірності та масштабу втрат), сучасних статистичних підходів (моделювання розподілів втрат, Value-at-Risk) та набору якісних інструментів (експертні оцінки, сценарії, аналіз першопричин тощо), а також їхні комбінації у змішаних підходах для формування цілісного ризикового профілю фінансової установи. Обґрунтовано, що кількісний підхід забезпечує вимірюваність і порівнянність результатів, але його застосовність обмежена якістю та достатністю історичних даних; якісний підхід дозволяє виявляти та оцінювати специфічні, у т.ч. нефінансові прояви ризику, проте має суб'єктивний характер; змішаний підхід поєднує переваги обох, забезпечуючи баланс між статистичною точністю і експертною інтерпретацією отриманих результатів. Зроблено висновки, що ефективне управління операційним ризиком вимагає інтеграції кількісних, якісних та змішаних підходів у систему управління операційними ризиками: кількісні моделі, зокрема дають основу для вимірювання фінансових втрат на основі історичних даних, якісні методи заповнюють прогалини історичних даних і виявляють новітніх проявів ризику (emerging risks), а змішані підходи забезпечують зрозумілі для стейкхолдерів консолідовані результати, які трактують отримані кількісні оцінки у відповідності до визначених діапазонів. Рекомендовано впроваджувати інтегровані підходи щодо оцінки операційного ризику комплексні з метою підвищення якості управлінських рішень і стійкості фінансової установи. Майбутні дослідження у сфері підходів оцінювання операційного ризику у фінансових установах мають бути спрямовані на розробку стандартизованих підходів до нормалізації даних, їх агрегування та зовнішнього бенчмаркінгу, на поглиблене вивчення гібридних методологій для досягнення балансу між статистичною точністю та експертною інтерпретацією, а також на проведення довгострокових досліджень щодо впливу новітніх ризиків на стійкість фінансових установ в умовах геополітичної нестабільності та технологічних трансформацій.*

Ключові слова: *операційний ризик, оцінка операційного ризику, кількісні підходи, якісні підходи, змішані підходи.*

Формул: 3, рис.: 3, табл.: 4, бібл.: 25

Abstract. *The article examines approaches to assessing operational risk in financial institutions, with an emphasis on quantitative, qualitative and hybrid methods in the context of rising uncertainty driven by military, geopolitical, technological and regulatory factors. Theoretical foundations of traditional metrics (the product of probability and loss severity), contemporary statistical approaches (loss distribution modeling, Value at Risk) and a set of qualitative instruments (expert judgment, scenario analysis, root-cause analysis, etc.) are considered, as well as their combinations within hybrid approaches for constructing a comprehensive risk profile of a financial institution. It is argued that the quantitative approach provides measurability and comparability of results but its applicability is constrained by the quality and sufficiency of historical data; the qualitative approach enables identification and assessment of specific risk events including non-financial ones, but is inherently subjective; the hybrid approach combines the strengths of both, striking a balance between statistical precision and expert interpretation of results. The advantages and limitations of modern methods (LDA, VaR) are demonstrated, notably their capacity to quantify aggregate risk while offering limited direct support for decision-making at the level of individual processes. The study concludes that effective operational risk management requires integration of quantitative, qualitative and hybrid approaches into the operational*

risk management framework: quantitative models provide a basis for measuring financial losses using historical data, qualitative methods fill gaps in historical records and reveal emerging risks, and hybrid approaches deliver consolidated, stakeholder-comprehensible outputs that contextualize quantitative estimates within defined ranges. The paper recommends implementing integrated assessment practices, including data normalization and aggregation, model validation, sensitivity analysis and result visualization, to improve the quality of managerial decisions and enhance the resilience of financial institutions. Future research of operational risk assessment approaches in financial institutions should advance standardized approaches to data normalization and benchmarking, refine hybrid methodologies that balance statistical precision with expert interpretation, and conduct longitudinal studies on emerging risks and institutional resilience under geopolitical and technological transformation.

Keywords: *operational risk, operational risk assessment, quantitative approaches, qualitative approaches, hybrid approaches.*

Formulas: 3, fig.: 3, tab.: 4, bibl.: 25

Introduction. The rising level of uncertainty, driven by factors including the war in Ukraine, geopolitical and globalization challenges, technological transformations, and regulatory changes, significantly impacts the operations of financial institutions at both national and international levels. Under these conditions, operational risk assessment becomes a determinant of managerial decision-making and an organization's ability to achieve its strategic and operational objectives.

Despite substantial progress in the development of risk management scientific theory and practice, the academic literature still lacks a unified approach to the interpretation of operational risk and the establishment of fundamental requirements for its assessment. The dominance of quantitative methods, particularly loss modeling based on historical data, has facilitated the development of tools for constructing integrated risk profiles of financial institutions.

At the same time, these approaches remain insufficiently integrated with qualitative and mixed-method assessment techniques. This limitation constrains the effectiveness of operational risk management systems, as quantitative models do not provide a comprehensive basis for identifying and evaluating specific risk occurrences, especially those not captured in historical datasets. Furthermore, they fail to account for the perception and scale of operational risk events that do not result in direct financial losses.

In this context, the development of a comprehensive approach to operational risk assessment, one that reflects the diverse nature of its occurrences and integrates both quantitative and qualitative methods, becomes particularly relevant and needed.

Literature review. Considering the trends in the development of the global economy, particularly globalization processes, changes in information flows, and the evolving perception of such information by stakeholders, there has been a growing focus on the management of operational risks within organizations. These tendencies are reinforced by the increasing number of disclosures made by various institutions regarding the impact of operational risk occurrences on the intended course of their activities.

In recent years, numerous high-profile operational risk events have been documented across various industries, demonstrating the diverse nature and systemic impact of such risks. Notable examples include unauthorized trading activities at Societe Generale, resulting in losses of €4.9 billion (Pichet, 2010); large-scale payment card data breaches at Target (BBC News, 2013; Plachkinova & Maurer, 2018); increasing injury rates in Amazon warehouses (Strategic Organizing Center, 2025); manipulation of emissions data by Volkswagen (Jung & "Alison" Park, 2017); the Fukushima Daiichi nuclear disaster triggered by a natural catastrophe (Polleri, 2025); a data center outage at Delta Airlines that caused the cancellation of over 2,000 flights (Mullen, 2017); and deficiencies in Boeing's internal control systems during the development of the 737 MAX aircraft, which contributed to multiple aviation accidents (Kuczynski et al., 2021). These events demonstrate that operational risk is an inherent and unavoidable component of business activity across all industries.

A considerable body of domestic and international research has been devoted to the theoretical aspects of operational risk management, particularly in relation to the identification of its occurrences, the evaluation of their consequences, the decision-making processes regarding appropriate responses, and the functioning of monitoring systems designed to detect deviations from the intended course of organizational processes. These issues are addressed in the works of scholars such as N. Sokolovska, who emphasizes the systemic nature of operational risk, noting its close interconnection with other risks inherent in banking activities and its potential role as a trigger for their realization (Sokolovska, 2022). N. Sokolovska also explores the aspects of enhancing risk culture and awareness regarding operational risks, which serves as a foundation for improving operational risk management practices within the banking sector (Sokolovska, 2022).

H. Yevtushenko, A. Baboshko, and D. Bushlia, in turn, examine the main directions for improving operational risk management systems in banking institutions through the application of both quantitative and qualitative tools for assessing the level of operational risk (Yevtushenko et al., 2015). O. Naumova and A. Kopyl propose integrating approaches to personnel auditing into the operational risk management framework of organizations in order to enhance the effectiveness of their internal control systems (Naumova & Kopyl, 2025). Within the context of recent trends in the dissemination of artificial intelligence technologies, D. Bezshtanko analyzes potential avenues for employing such tools in tasks related to the identification, preliminary assessment, and development of managerial response options to operational risk occurrences detected by artificial intelligence algorithms (Bezshtanko, 2025).

As can be observed, scholarly interest in specific aspects of operational risk management remains consistently high. At the same time, the universal nature of operational risk and the broad spectrum of issues associated with its management provide a solid foundation for further research.

Aim and Methodology. The aim of this article is to compare approaches to the assessment of operational risk in financial institutions and to substantiate the theoretical and methodological foundations for their integration into the operational risk management system of such institutions.

To achieve this aim, the study employed a structured combination of general scientific and specialized research methods, each serving a distinct analytical function:

Analysis and synthesis – applied to deconstruct existing definitions of operational risk and reconstruct a consolidated authorial definition. This method allowed identification of common elements across academic, regulatory, and institutional perspectives, followed by synthesis into a unified conceptual framework.

Comparative analysis – used to contrast quantitative, qualitative, and mixed approaches, highlighting their advantages, limitations, and applicability. For example, traditional probability & impact models were compared with modern loss distribution approaches (LDA, VaR), while qualitative expert-based tools were contrasted with hybrid interpretations.

Systems approach – ensured that operational risk was examined not as isolated events but as part of the broader risk management system of financial institutions. This method emphasized interconnections between processes, controls, and managerial decision-making framework of the financial institution.

Process approach – focused on operational risk as deviations from the target course of institutional processes. This allowed classification of risks according to their impact on process outputs and facilitated integration of assessment methods into process-based management.

Logical-structural analysis – applied to organize the classification of approaches (Table 1) and to build a coherent narrative linking definitions, methodological tools, and managerial implications. This method provided the basis for structuring the article's results and conclusions.

Results. Given the significant attention to operational risk from regulators, international organizations, and academia, there is a need for a unified definition as a foundation for further analysis.

A distinctive feature of the development of the concept of operational risk is its origin within the risk management frameworks of financial institutions, largely driven by the Basel Committee's publications (Basel Committee on Banking Supervision, 1998; 2001). The 1998 publication is considered a "starting point" due to its explicit reference to operational risk as an integral component of the "risk universe" accompanying the activities of financial institutions.

To highlight the perspectives of academic schools, international organizations, and regulators, a comparative analysis of the concept of "operational risk" is required. For example, N. Sokolovska defines operational risk as the uncertainty of adverse economic outcomes of a bank's activities (losses, damages, or foregone income) arising from internal failures or external factors, including human actions, system disruptions, and process deficiencies (Sokolovska, 2022).

At the same time, S. Ashby argues that operational risk reflects the impact of unforeseen outcomes on the efficiency and effectiveness of operations (Ashby, 2022). D. Tattam expands the definition of operational risk by including not only losses but also potential gains arising from people, systems, or external events that may cause an organization to deviate from its objectives (Tattam, 2011).

The National Bank of Ukraine provides its own definition of operational risk as the probability of incurring losses, additional damages, or failing to achieve planned income due to shortcomings or errors in the organization of internal processes, intentional or unintentional actions of bank employees or other persons, failures in banking systems, or the influence of external factors. According to the National Bank of Ukraine, operational risk encompasses legal risk, model risk, information security risk, and ICT risk, while excluding reputational and strategic risk (National Bank of Ukraine, 2018).

To establish a universal definition of operational risk, the specifics of managerial decision-making based on goal setting within financial institutions must be considered. Strategic objectives become tactical and operational goals that consider resource allocation and competency development. Management establishes these objectives as targets for functional areas, process groups, and core business processes.

The processes of a financial institution constitute the core mechanisms for transforming resources to meet the needs of external or internal clients (i.e., the creation of process outputs) in accordance with established procedures. The formalized sequence of such transformations defines the target state of processes, which serves as the primary object of operational risk management.

Based on the above, we propose defining operational risk as the degree of negative deviation from the expected outcome of the target course of a financial institution's process (the process output). This definition considers exclusively the negative form of deviation from the target course of processes, expressed in the form of unplanned losses or expenses of the institution, since positive deviations represent the realization of opportunities rather than risk in its general sense (Samad-Khan et al., 2006).

Given that financial institutions always operate under conditions of uncertainty, the expected and actual results of their activities, shaped by external and internal factors, will inevitably vary. The task of assessing the scale of influence of these factors on deviations from the target course of processes requires the implementation of quantitative, qualitative, and mixed approaches to evaluating such deviations as occurrences of operational risk.

Considering the necessity of classifying approaches to operational risk assessment in financial institutions, we propose an authorial approach, detailed in Table 1.

Table 1

Classification of Approaches to Operational Risk Assessment in Financial Institutions

Category of Approach to Operational Risk Assessment	Definition of Approach to Operational Risk Assessment	Examples of Application of Operational Risk Assessment Approaches
Quantitative	Based on the analysis of numerical datasets, statistical models, and indicators, this approach aims to measure the probability of occurrence and/or the materiality of the consequences of operational risk	- Assessment of actual losses incurred as a result of operational risk occurrences. - Estimation of the overall volume of operational risk requiring capital coverage. - Evaluation of potential losses resulting from operational risk occurrences.
Qualitative	Grounded in expert judgment and the interpretation of non-numerical information, this approach seeks to form evaluative insights into the perception of operational risk.	- Assessment of operational risk level inherent in a single occurrence (e.g., "High," "Medium," "Low"). - Qualitative evaluation of operational risk trends (e.g., "Increasing," "Decreasing," "Stable").
Mixed	Focused on the qualitative interpretation of results derived from the analysis of numerical datasets, this approach ensures a balance between statistical accuracy and the perception of risk levels.	- Assessment of operational risk level based on predefined triggers or ranges (e.g., "0–100 units – Low," "101–200 units – Medium"). - Consolidation of expert judgment data (e.g., "62% of experts assessed the occurrence of operational risk as High").

Source: Compiled by the author

Considering the specific nature of operational risk, assessment approaches provide insights into the volume of risk (quantitative approaches) and the level of risk (qualitative and mixed approaches). We propose examining these approaches to operational risk assessment in accordance with the authorial classification presented.

For the purpose of quantitative assessment of the volume of operational risk, scholars apply the traditional and modernized approaches.

The traditional approach, according to its assumptions, defines the volume of operational risk as the product of the likelihood of occurrence and the impact of its consequences.

$$Risk = Likelihood \times Impact, \quad (1)$$

where Likelihood – the estimated likelihood of occurrence of a specific operational risk incident (expressed as a percentage) and Impact – the estimated level of losses faced by the organization in the event of a specific operational risk incident (expressed in monetary units).

Thus, the traditional approach to assessing the volume of operational risk is based on the analysis of the outcomes of individual hypothetical operational risk incidents.

The modernized approach defines operational risk as the volume of loss under a given level of uncertainty. According to this approach, if the probability of loss realization is 100% (that is, the loss is inevitable), the risk volume is considered to be zero. The principal distinction of the modernized approach to operational risk management lies in the examination of a specific class of risk events using frequency and severity distribution indicators.

Visualization of these approaches and interpretation of the results of their application are presented in Figure 1:

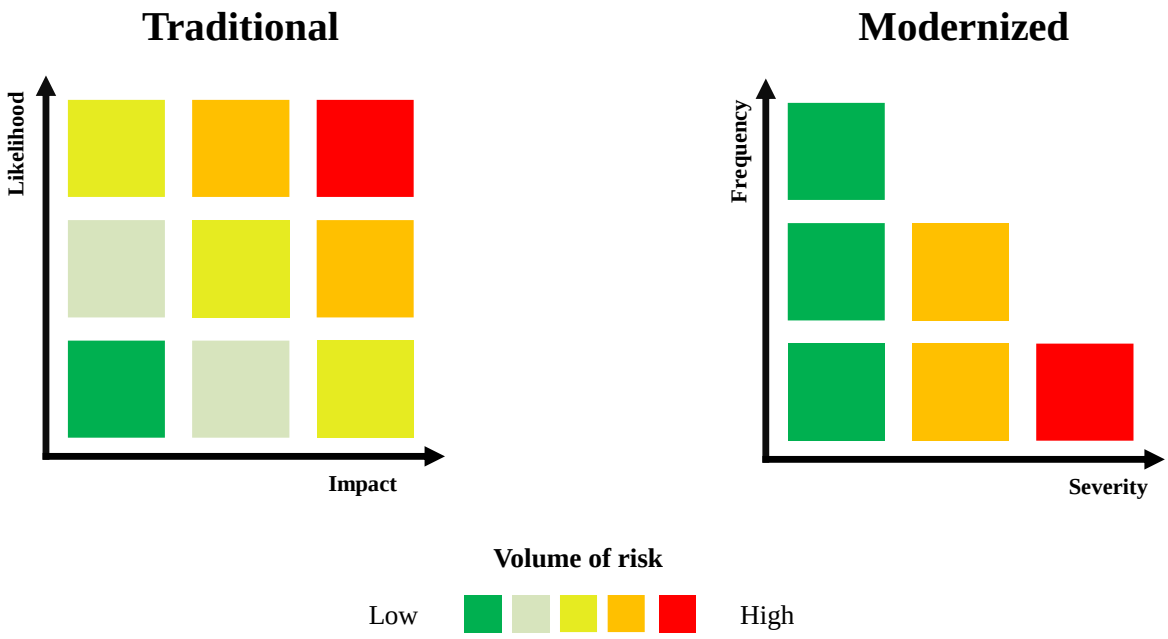

Figure 1. Traditional and Modernized Approaches to Operational Risk Volume Assessment

Source: (Samad-Khan, 2010)

Within the paradigm of the traditional approach to operational risk volume assessment, the concepts of expected losses and unexpected losses are employed. Expected losses are understood within this approach as the consequences of operational risk events characterized by low impact and high likelihood of occurrence. Unexpected losses are understood as the consequences of operational risk events associated with high impact (Pescaroli et al., 2025).

The examined approach to assessing the volume of operational risk by obtaining the product of the likelihood of occurrence and the impact of losses from individual operational risk events of the organization, in accordance with the traditional approach, has its advantages and disadvantages.

The main advantages of this approach include: (1) computational simplicity, based on the product of the probability of occurrence and the associated loss impact; (2) comparability across different operational risk events; (3) the ability to rank risk events by estimated impact; and (4) the development of qualitative scales for risk assessment (e.g., low, medium, high).

This approach has the main disadvantages: (1) limited availability of internal data on operational risk events, particularly those not previously observed or insufficiently recorded; and (2) the implicit assumption of events with a certain probability and catastrophic impact. Such assumptions lack empirical validity, as events of this nature are extremely rare and preclude the accumulation of statistical evidence, thereby undermining their justification within the traditional framework.

Thus, the traditional approach to assessing operational risk volume is more suitable for parameterizing individual operational risk events within a financial institution than for assessing the overall volume of operational risk to which the institution is exposed.

In contrast, within the modernized approach to operational risk volume assessment, similar operational risk events with significant impact are classified as low-frequency, high-severity events. The frequency of operational risk events, considered as an empirical rather than a theoretical measure, serves as the basis for calculating the impact of the so-called expected loss resulting from the realization of operational risk events.

Accordingly, under the modernized approach to operational risk volume assessment, there are no operational risk events within a financial institution's activities that occur frequently and simultaneously have a high level of severity. For the classification of operational risk events with low frequency of occurrence and high severity, the unexpected loss category is applied, which, within this concept, is equivalent to the notion of risk. A comparison of traditional and modernized approaches to defining expected and unexpected losses from operational risk events is presented in Table 2.

Table 2

Comparative Analysis of the Essence of "Expected" and "Unexpected" Losses Resulting from Operational Risk Events within the Traditional and Modernized Approaches to Operational Risk Volume Assessment

Approach to Operational Risk Volume Assessment	Expected losses	Unexpected Losses
Traditional Approach	Minor losses with high likelihood of occurrence	Major losses with low likelihood of occurrence
Modernized Approach	Not applicable	

Source: generalized by the author based on Samad-Khan (2010)

Within the modernized approach to operational risk volume assessment, the concept of expected loss is an empirically derived measure calculated as the average value of losses weighted by the probability of operational risk events.

The concept of unexpected loss represents the difference between the loss value of operational risk events at a given confidence interval (for example, 95% or 99.9%) and the average loss value weighted by the probability of occurrence of operational risk events (the "expected loss").

The consequences of operational risk events beyond the confidence interval within the modernized approach are defined as catastrophic loss.

The concepts of "expected loss," "unexpected loss," and "catastrophic loss" are illustrated in the graphical representation (Figure 2).

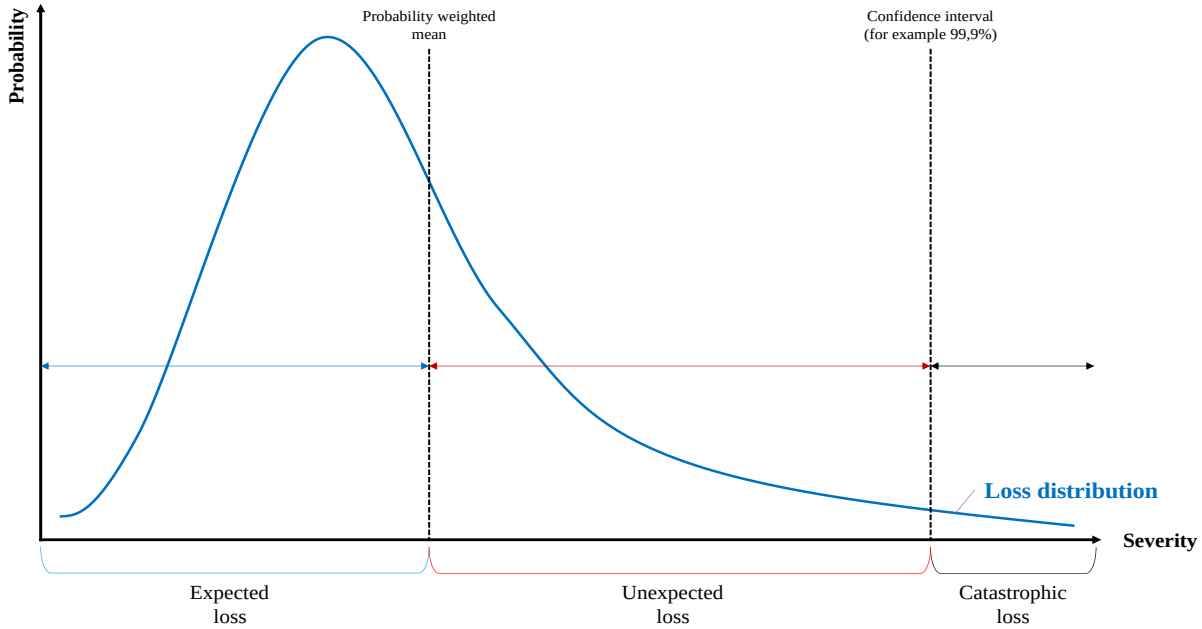

Figure 2. Expected, Unexpected, and Catastrophic Loss under the Modernized Approach to Operational Risk Volume Assessment

Source: generalized by the author based on Jobst (2007) and Samad-Khan (2010)

The modernized approach, in turn, is based on the Loss Distribution Approach (LDA), the main principle of which lies in dividing the dataset of risk events into segments that address the following questions:

1.How frequently do these events occur (what is the frequency of identification of risk event?

2.What losses accompany them (what is the severity of risk events)?

By segmenting the dataset of operational risk events under analysis, the number of observation points is effectively doubled (Chapelle et al., 2005).

The Loss Distribution Approach includes the following key elements:

Event frequency: a discrete distribution based on the number of operational risk events within a given period of time, usually one year. The frequency of operational risk events is most often modeled using the Poisson distribution.

A discrete random variable X as a Poisson distribution with parameter $\lambda > 0$, if, for $k = 0, 1, 2...$ the probability mass function of $X$is defined as follows:

$$f(k;\lambda) = \Pr(X = k) = \frac{\lambda^k e^{-\lambda}}{k!} \quad (2)$$

Where:

e – Euler's number (2,71828…)

$k!$ – factorial of k

The positive real number λ is equal to both the expectation and the variance of X:

$$\lambda = E\,(X) = Var\,(X) \quad (3)$$

Where:

$E\,(X)$ – expectation of X

$Var\,(X)$ – variance of X

Event severity: a continuous distribution, asymmetric and heavy-tailed, the application of which is determined by the dual nature of the distribution of operational risk events, namely: a large number of events with small losses and a relatively small number of events with significant losses.

The most common approach to modeling event severity is the lognormal distribution, obtained by transforming the normal (Gaussian) distribution via the logarithm. Additionally, the Weibull distribution and the Generalized Pareto Distribution (GPD) are employed to model the severity distribution of operational risk events.

Within the Loss Distribution Approach (LDA), the modeled distributions of frequency and severity of operational risk events are consolidated into an aggregated loss distribution from operational risk events (Figure 3).

The most widely used consolidation method today is the Monte Carlo method, according to which the aggregated loss distribution from operational risk events is generated through one million (or more) random simulations of the dataset describing the severity of operational risk events and the frequency of their occurrence.

Other methods for modeling the consolidated loss distribution resulting from operational risk events, such as the Fast Fourier Transform (FFT) and Panjer Recursion, are based on equations that require time for model preparation (parameterization) and mathematical substantiation of their parameters, while at the same time allowing less time to be spent on the actual computation.

The assessment of operational risk volume under the indicated approach is essentially an adaptation of the Value-at-Risk (VaR) methodology, which aims to provide an estimate of the potential loss amounts of an organization (both expected and unexpected) resulting from the realization of risk events over a defined time horizon.

In practice, the Value-at-Risk with a 99.9% confidence interval reflects the calculated amount of organizational losses that should not exceed a certain threshold with a probability of 99.9% over the specified time horizon.

The application of this approach in the context of risk management, from a mathematical perspective, involves constructing an organization's loss distribution in accordance with the investor's expectations or risk profile (Chaudhuri & Ghosh, 2016).

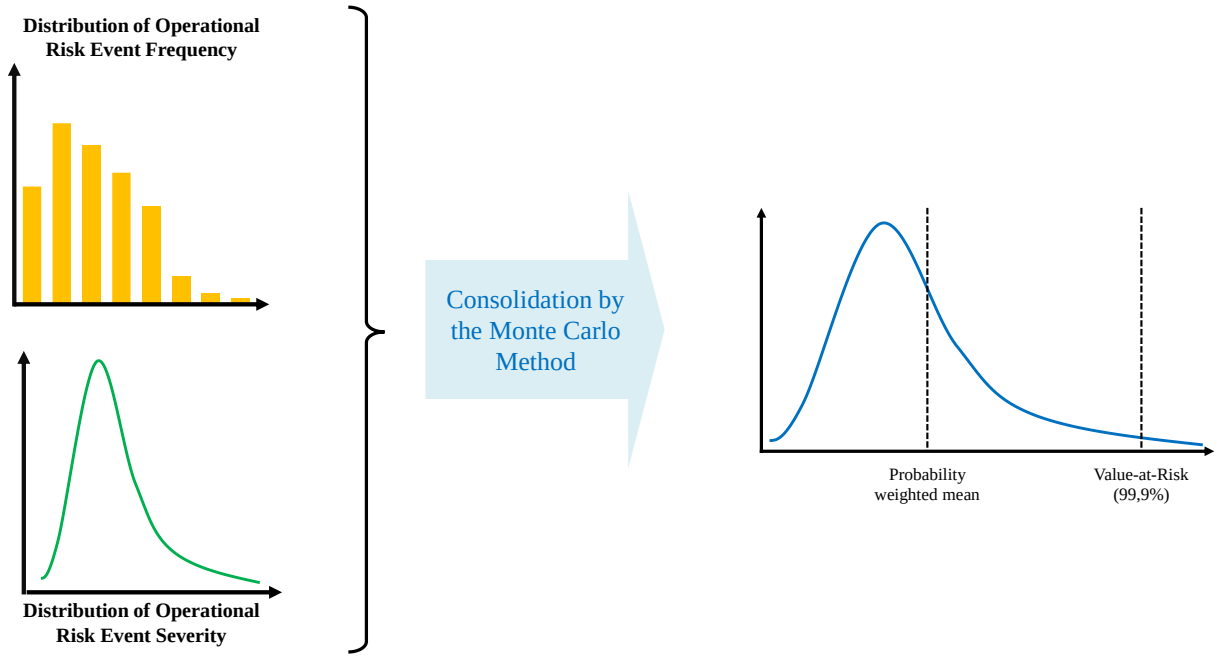

Figure 3. Consolidation of Frequency and Severity Distributions of Operational Risk Events

Source: generalized by the author based on Chapelle (2019), Jobst (2007), and Samad-Khan (2010)

The considered approach to operational risk volume assessment, based on organizational loss modeling using the Value-at-Risk methodology, has its advantages and disadvantages.

The main advantages of this approach include: (1) the provision of a clear and quantitatively measurable estimate of potential losses from operational risk events; and (2) the ability to compare indicators over time for managerial decision-making and performance evaluation.

The main limitations include: (1) the requirement for substantial input data for modeling; and (2) reliance on historical distributions of the frequency and severity of operational risk events.

Thus, the quality of operational risk assessment under the Value-at-Risk (VaR) approach depends primarily on: (1) the sufficiency of internal data on past operational risk events, which, however, do not capture changes in processes, controls, organizational structure, or business models; (2) the availability of relevant external data on operational risk events from comparable financial institutions; and (3) access to information on changes in the operating environment, including regulatory developments, market dynamics, technological progress, and shifts in societal priorities.

Accordingly, assessing operational risk volume by evaluating losses under the modernized approach provides a general view of the risk level within the financial institution. At the same time, it does not address how to identify, assess, and respond to operational risk events of different natures, nor which strategy should be applied to each specific identified risk event.

In order to complement the quantitative assessment of operational risk with approaches that focus on non-financial data and information regarding operational risk events not recorded in the historical activity of the financial institution, it is advisable to employ qualitative methods of operational risk assessment, as presented in Table 3.

Table 3

Approaches to Qualitative Assessment of Operational Risk in Financial Institutions

Approach	Description	Advantages of the Approach	Disadvantages of the Approach
Brainstorming	A guided group session in which participants generate the maximum possible number of potential operational risk events, identify their causes, and assess their impact on the financial institution. This approach is used for rapid identification of operational risk events and for forming a consensus expert evaluation of their level.	- Speed of idea generation - Engagement of participants with diverse perspectives - Formation of a preliminary understanding of operational risks inherent to a specific type of activity	- Potential dominance of individual participants - Lack of structured validation of results - Group biases
Structured / Semi-structured Interviews	Targeted conversations with employees / experts using a predefined or partially flexible questionnaire to identify process deficiencies or behavioral factors influencing the level of operational risk.	- Depth of information obtained - Possibility of clarifying responses - Identification of problems hidden from statistics	- Resource intensity - Dependence on the interviewer's qualifications - Subjectivity of responses
Delphi Method	Iterative anonymous surveys of experts, followed by aggregation of responses and repeated rounds to achieve consensus regarding the probability, impact, or priority areas of risk realization.	- Reduces group pressure - Allows for obtaining consistent assessments - Useful for forecasting	- Resource intensity and duration of the process - Dependence on the composition of the expert group - Risk of forming a "middle-level" consensus - Subjectivity of assessments - Possibility of decreased participant motivation
Checklists	Consolidation of responses from participants completing questionnaires that contain standardized lists of known operational risk events.	- Simplicity of application - Standardization of checks - Useful for maintaining an up-to-date list of processes of the financial institution	- Does not account for new (including potential) risk events (emerging risks) or context-specific risks - Risk of formalism - Limited analytical depth
Scenario Analysis	Modeling of unlikely but high-impact (stress) scenarios and assessing their effect on the financial institution's activities using expert judgment.	- Focus on operational risk events with low probability of occurrence but significant impact (including those not yet recorded in the financial institution) - Complements the strategic planning of the financial institution - Provides a basis for business continuity management	- High dependence on the quality of scenarios - Complexity of transforming qualitative assessments into quantitative indicators and their subsequent validation - Significant resource intensity
Root Cause Analysis	A systematic process of identifying the primary causes of operational risk events or deviations from target process performance.	- Aimed at identifying and assessing the scale of impact of the problem's source - Increases the effectiveness of corrective actions - Improves the long-term resilience of the financial institution	- May be labor-intensive - Risk of obtaining superficial conclusions without in-depth analysis - Requires a sufficient volume of data for deeper analysis
Ishikawa (Fishbone) Diagram	A visual tool for systematizing potential causes of operational risk events into categories such as personnel, infrastructure, processes, and external factors.	- Structured identification of causes of operational risk events - Simplicity of visualizing analysis results	- May overlook the influence of hidden factors - Depends on the completeness of the discussion
Bow-tie Diagram	A visual model that demonstrates the transformation of threats into operational risk events, illustrates preventive controls, and describes consequences along with mitigation measures.	- Intuitive visualization - Useful for communicating operational risk events - Demonstrates preventive measures (controls) and the impact of operational risk events	- Limited accuracy of results - Excessive simplification of complex chains of operational risk event realization - Dependence of results on the quality of input data

Source: generalized by the author based on (Popov et al., 2022)

The mentioned approaches to the qualitative assessment of operational risk levels in a financial institution can be applied independently or in various combinations. Qualitative approaches to assessing operational risk levels make it possible to consider the specific features of the organizational structure, business model, and strategic objectives of the financial institution, even in the absence or incompleteness of numerical (quantitative) estimates of the operational risk exposure faced by the institution as a whole or by individual business lines. An additional advantage of qualitative approaches to assessing operational risk levels in a financial institution is the consideration of behavioral factors of its personnel, which are difficult to quantify. At the same time, when applying qualitative approaches to operational risk assessment, factors such as the subjectivity of evaluative judgments, the professionalism of participants, and the completeness of the issues under consideration should be considered. Furthermore, to assess operational risk levels in a financial institution, mixed approaches combining quantitative and qualitative methods are used. The main feature of these approaches is the assessment of operational risk levels within predefined ranges of evaluative judgments, based on analyses of numerical data sets. Given the specific occurrences of operational risk in a financial institution's activities, we propose the following high-level categorization of the key mixed approaches (Table 4).

Table 4

Key mixed approaches to assessing operational risk levels in financial institutions

Approach	Description	Advantages of the Approach	Disadvantages of the Approach
Analysis of operational risk indicator dynamics	This approach involves examining time series of key metrics of operational risk occurrences (both individual and consolidated) with the aim of identifying trends, seasonality, structural changes, and early warning signals of shifts in the operational risk level to which the financial institution is exposed. The approach combines statistical methods (trend analysis, time series, regressions) with expert interpretation of the causes and consequences of these changes.	- Enables the identification of early warning signals of adverse changes in the level of operational risk - Provides a basis for evaluating the effectiveness of measures taken over time - Allows forecasting of changes in the level of operational risk	- Depends on the quality and frequency of data collection and processing - May produce false signals in the case of short samples or structural changes - Requires methods for correcting seasonality and autocorrelation - Requires parameterization in the context of observation frequency and threshold/target values of the operational risk level
Structural analysis	This approach is aimed at detailing the operational risk profile by components in which its impact is occurred (processes, departments, geographical distribution, organizational units, event types, etc.), in order to identify concentrations, root causes of risk occurrence, and interconnections among these elements.	- Identifies concentrations and “bottlenecks” - Helps determine priority areas for detailed analysis and the implementation of measures	- Requires a consistent classification of events, processes, business lines, and data normalization - Creates a risk of excessive aggregation, which may conceal local issues
Combined analysis (dynamics of structure)	An integrated approach combines the analysis of indicator dynamics with their structural distribution to assess how the structure of operational risk occurrences/metrics evolves over time (for example, an increasing share of a certain type of events or a shift of risk concentrations toward a specific business line).	- Provides a comprehensive understanding of the evolution of the risk profile - Useful for identifying transformational risks and risks related to strategic planning	- High requirements for data quality and methodological consistency in interpreting the results of their consolidation and analysis - Complexity of interpretation in the case of multidimensional changes

Source: developed by author

Since the key feature of mixed approaches to assessing operational risk levels in financial institutions is the use of both quantitative and qualitative data, researchers and practitioners face the challenge of developing an additional system of requirements for the formation and interpretation of the results of such analysis.

Additional tasks aimed at addressing the outlined challenges include:

1.Application of aggregation and normalization methods – a set of procedures and rules for transforming and comparing quantitative and qualitative indicators of operational risk, as well as their aggregation into consolidated indicators. Normalization is intended to align measurement scales (e.g., creating intervals or ranges). At the same time, aggregation provides tools for combining normalized components, accounting for their weights and correlations, to form integrated indices or ratings.

2.Application of attribution analysis – to distribute assessments of the contribution of individual components of operational risk (personnel, processes, infrastructure, external factors). The purpose of this approach is to quantitatively or qualitatively determine each factor's contribution to the overall change in the operational risk profile using regression models, index systems, or expert evaluations.

3.Application of validation and verification methods – aimed at testing the adequacy, reliability, and applicability of models and results of operational risk level/volume assessment in a financial institution. These include back-testing (checking forecasts against historical data), scenario testing (modeling conditions of scenario realization and assessing the scale of consequences), and independent expert review of obtained results (verification of assumptions regarding operational risk level/volume assessment by external or internal experts).

4.Consideration of uncertainty in statistical and empirical methods of quantitative assessment of operational risk level/volume. This includes sensitivity analysis (determining how changes in model parameters affect results), construction of confidence intervals for estimates, and bootstrap methods for evaluating distributions and stability of indicators under limited input data.

5.Visualization of obtained results – application of graphical methods to represent the dynamics, structure, and interconnections of operational risk indicators. These approaches aim to visually present the concentrations or intensities of indicators or “problem areas” identified in the assessment of operational risk level/volume (so-called “heat maps”), illustrate flows of information, values, or resources, and demonstrate time trends of aggregated operational risk indices.

Accordingly, mixed approaches to operational risk assessment provide a foundation for managerial decision-making that goes beyond processing numerical data sets or expert judgments, to more explicitly structure and visualize the available data.

Conclusions. In our view, quantitative approaches to operational risk assessment in financial institutions should be complemented by qualitative and mixed methods. This integration enables the mitigation of data limitations, the modeling of previously unobserved risk events, the structuring of data into evaluative ranges, the visualization of analytical results, and the identification of trends in the dynamics and structure of operational risk indicators.

The application of a comprehensive approach to operational risk assessment, which incorporates the methods described above as well as other applicable techniques, should ensure both the completeness of the analysis and the ease with which stakeholders perceive the institution’s operational risk profile.

Furthermore, when comprehensive and readily interpretable risk-profile information is integrated into the governance and decision-making processes of management and owners, it underpins the prudence of managerial decisions and contributes to the long-term stability and resilience of the financial institution.

Future research of operational risk assessment approaches in financial institutions should focus on several key directions. First,

the development of standardized approaches to data normalization, aggregation, and external benchmarking remains an open challenge that warrants comparative research across jurisdictions and financial institutions with different business models. Second, further exploration of hybrid methodologies is needed to refine the balance between statistical precision and expert interpretation, with emphasis on visualization techniques that improve stakeholder comprehension. Finally, longitudinal studies examining the emerging risks and their impact on resilience of financial institutions under conditions of geopolitical instability and technological transformation would provide valuable insights into the adaptability of operational risk assessment approaches.

Conflict of Interest. The author declares that the research was conducted in the absence of any commercial or financial relationships that could be interpreted as a potential conflict of interest.

Funding. The author states that no specific funding was received for the publication of this article.

Ethical Statement. All procedures carried out within the scope of this study adhered to institutional and international ethical standards.

Generative AI Statement. The author confirms that generative artificial intelligence was not utilized in the preparation of this manuscript.

Acknowledgments. The author expresses sincere gratitude to Mrs. Olena Naumova, Ph.D. in Economics, Associate Professor of the Department of International Business («KROK» University, Kyiv, Ukraine) for valuable guidance and to colleagues for constructive feedback. The author also thanks family members for their encouragement.

References:

1)Євтушенко Г.В., Бабошко А.І., & Бушля Д.І. (2015). *Євтушенко Г.В., Бабошко А.І., Бушля Д.І. Операційні ризики в системі банківської діяльності та нові шляхи їх попередження*. http://global-national.in.ua/issue-5-2015/13-vipusk-5-traven-2015-r/821-evtushenko-g-v-baboshko-a-i-bushlya-d-i-operatsijni-riziki-v-sistemi-bankivskoji-diyalnosti-ta-novi-shlyakhi-jikh-poperedzhennya

2)Наумова, О., & Копил, А. (2025). РОЛЬ КАДРОВОГО АУДИТУ В СИСТЕМІ УПРАВЛІННЯ РИЗИКАМИ ОРГАНІЗАЦІЇ: ВПЛИВ НА ЛОЯЛЬНІСТЬ ПРАЦІВНИКІВ. *Сталий розвиток економіки*, (1 (52)), 288–296. https://doi.org/10.32782/2308-1988/2025-52-40

3)Національний банк України. (2018). *Положення про організацію системи управління ризиками в банках України та банківських групах*.

4)Соколовська, Н. (2022). *ОПЕРАЦІЙНИЙ РИЗИК-МЕНЕДЖМЕНТ У БАНКАХ*. Київський національний економічний університет імені Вадима Гетьмана.

5)Ashby, S. (2022). *Fundamentals of Operational Risk Management: Understanding and Implementing Effective Tools, Policies and Frameworks*. Kogan Page, Limited.

6)Basel Committee on Banking Supervision. (1998). *Operational Risk Management*.

7)Basel Committee on Banking Supervision. (2001). *QIS 2—Operational Risk Loss Data*.

8)BBC News. (2013). Target card heist hits 40 million. *BBC News*. https://www.bbc.com/news/technology-25447077

9)Bezshtanko, D. (2025). AI AND BANK'S OPERATIONAL RISK MANAGEMENT. *Three Seas Economic Journal*, *6*(2), 22–27. https://doi.org/10.30525/2661-5150/2025-2-4

10)Chapelle, A. (2019). *Operational risk management: Best practices in the financial services industry*. John Wiley and Sons, Inc. https://doi.org/10.1002/9781119548997

11)Chapelle, A., Crama, Y., Hubner, G., & Peters, J.-P. (2005). Measuring and Managing Operational Risk in the Financial Sector: An Integrated Framework. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.675186

12)Chaudhuri, A., & Ghosh, S. (2016). *Probabilistic View of Operational Risk* (Вип. 331, с. 47–73). https://doi.org/10.1007/978-3-319-26039-6_4

13)Jobst, A. (2007). Consistent Quantitative Operational Risk Measurement and Regulation: Challenges of Model Specification, Data Collection, and Loss Reporting. *IMF Working Papers*, *07*(254), 1. https://doi.org/10.5089/9781451868173.001

14)Jung, J. C., & "Alison" Park, S. B. (2017). Case Study: Volkswagen's Diesel Emissions Scandal. *Thunderbird International Business Review*, *59*(1), 127–137. https://doi.org/10.1002/tie.21876

15)Kuczynski, J., Wang, C., & Hoffman, F. (2021). Boeing 737 MAX: A case study of failure in a supply chain using system of systems framework. *Issues in Information Systems*, *22*, 51–62. https://doi.org/10.48009/1_iis_2021_51-62

16)Mullen, R. M., Jethro. (2017, Січень 30). *Computer outage grounds Delta flights in U.S. | CNN Business*.

CNN. https://www.cnn.com/2017/01/29/news/delta-system-outage

17)Pescaroli, G., McMillan, L., Gordon, M., Aydin, N. Y., Comes, T., Maraschini, M., Palma Oliveira, J., Torresan, S., Trump, B., Pelling, M., & Linkov, I. (2025). Definitions and taxonomy for High Impact Low Probability (HILP) and outlier events. *International Journal of Disaster Risk Reduction*, *127*, 105504. https://doi.org/10.1016/j.ijdrr.2025.105504

18)Pichet, E. (2008). What Governance Lessons Should be Learnt from the Société Générale's Kerviel Affair? *La revue Française de Gouvernance d'Entreprise*, 3, 117–138.

19)Plachkinova, M., & Maurer, C. (2018). Teaching Case Security Breach at Target. *Journal of Information Systems Education*, *29*(1). http://jise.org/Volume29/n1/JISEv29n1p11.html

20)Polleri, M. (2025). Fukushima and the Politics of Nuclear Disaster Recovery. *Current History*, *124*, 216–221. https://doi.org/10.1525/curh.2025.124.863.216

21)Popov, G., Lyon, B. K., & Hollcroft, B. (2022). *Risk assessment: A practical guide to assessing operational risks* (Second edition). John Wiley & Sons, Inc. https://doi.org/10.1002/9781119798323

22)Samad-Khan, A. (2010). *New approach of the operational risk management*. Society of Actuaries. https://www.soa.org/globalassets/assets/files/research/projects/research-new-approach.pdf

23)Samad-Khan, A., Rheinbay, A., & Le Blevec, S. (2006). *Fundamental Issues in OpRisk Management. OpRisk &Compliance*. https://www.sbp.org.pk/bsrvd/pdf/KnowledgeSharing/Reading%20Material%20for%20workshop%20on%20ORM%20May%2018-22,%202009/General%20Articles/Fundamental%20Issues%20in%20OpRisk%20Management.pdf

24)Strategic Organizing Center. (2025). F*ailure to deliver—Amazon falls short on safety*. Strategic Organizing Center. https://thesoc.org/resources/failure-to-deliver-amazon-falls-short-on-safety

25)Tattam, D. (Ed.). (2011). *A short guide to operational risk*. Gower.