

NEW TENDENCIES IN OPERATIONAL RISK MANAGEMENT IN BANKS: CHALLENGES AND OPPORTUNITIES

Jelena Sobanova¹

University of Latvia, Faculty of Business, Economics and Management

Marina Kudinska²

University of Latvia, Faculty of Business, Economics and Management

Abstract

The importance of operational risk management in the bank increases every year. Banks need to take actions to prevent fraudulent activities, minimize errors in transactions, automate processes and improve data security. Ignoring operational risk procedures or failure to implement suitable control mechanisms could lead to unexpected losses, unsatisfied customers, and potentially regulatory sanctions, all of which could seriously harm bank's reputation in a highly competitive market. A specific focus is on payments and security transactions, as they are linked to the biggest risks. Any regulatory driven project failure or IT project failure in the bank, insufficient project governance, failed implementation of a new system or failure in external data sources can lead to even bigger losses. After a review of the Basel Framework and the new set of standards of the upcoming changes to take effect as of 2023, the aim of this article is to elucidate the changes related to operational risk capital in banks and to ascertain the weakest points in operational risk management. Therefore, this topic is timely relevant, as the aim of the research is to manifest the possible changes withing operational risk management in banks, by gathering and analysing empirical evidence. This article is based on academic research and professional experience. The methods used in the research are comparison, generalization and graphical illustration of statistical information, identification of the main idea of regulatory frameworks and legal documentation. The main results and findings of the research are that banks will need to rethink the strategies of their capital management and this article emphasizes the importance of a redesigned approach towards operational risk assessment in Basel III and substantiates the efficiency of the proposed framework. With Basel III, each loss may cause more challenges, as will be considered twice, as the direct impact on profit/loss and direct impact on future operational risk capital. Another finding is that the biggest amounts of losses are related to corporate items events and according

¹ **Contact:** Jelena Sobanova; Jelenasobanova@gmail.com; Faculty of Business, Management and Economics, University of Latvia, Aspazijas bulvaris 5, Riga, LV-1050, Latvia

² **Contact:** Marina Kudinska; Marina.Kudinska@lu.lv; Faculty of Business, Management and Economics, University of Latvia, Aspazijas bulvaris 5, Riga, LV-1050, Latvia

to the static data taken from ORX membership community, top five monthly losses are far from normal distribution. Important finding was that most of the banks were not prepared for COVID-19-pandemic and had to review operational risk procedures immediately to secure their business in working from home environment, meaning that gap in operational risk management existed already before COVID-19-pandemic.

Key words: bank operational risk, operational risk management.

Introduction

Operational risk plays a meaningful role in any field, for instance, mechanical failure in the shipping industry, a mistake in medicine, a human error in engineering, an incorrect decision in law and economics, as human factors may result in a process failure, losses or even person's death.

Although operational risk is not a new area of research, the meaning of the definition has raised concerns about operational risk management, and its official definition was proposed by Basel II in 2001, stating that it is "the risk of loss resulting from inadequate or failed internal processes, people and systems or from external events". Furthermore, banks are heavily affected by the mandatory regulations of the Basel Framework. Even though Basel III became effective in 2019, some important elements such as the revised operational risk framework should be implemented by 2023.

To form operational risk capital, banks need to analyse their operational risk appetite. Legal aspects of operational risk are recorded in the Basel Accords, which require banks to calculate minimum operational risk capital using different approaches.

The aim of this article is to shed light on the changes within the Basel framework, as operational risk capital in banks must be calculated using the Revised Standardized Approach (RSA) for operational risk, also called the Standardised Measurement Approach (SMA). All banks are required to use only this approach, which factors in historical operational risk losses as well as business indicator components (BIS, 2019).

Thus, the main research questions posed in this study are the following: *To examine the changes related to the regulations, why are there changes in the regulation and what are the main factors impacting operational risk capital? The effect and challenges of operational risk management and the impact on operational risk capital after these changes. What are the riskiest processes in banks and how to minimize the biggest losses?* The study findings are expected to contribute to ascertaining general gaps of operational risk management and could be used for further evidence to highlight the importance of operational risk management in banks, as well as the necessity of long-term planning of operational risk capital, establishing control procedures and timely collected data for the incident losses in the past.

Literature review

To conduct the assessment of the topic presented, the authors used different sources for the literature review. This article is developed by using theoretical, scientific and specialized articles from academic journals, O.R.X. member reports, European and international legal documents and working papers, Basel Committee on Banking Supervision regulatory frameworks and reports, European Central Banks reports, UK Financial Services Authority reports, Latvian Central bank's reports.

The existing literature emphasizes the relationships between operational risk management and operational risk capital. Earlier work, including Harmantzis F. (2003) and Froot T. (2003) provided critical aspects of operational risk management frameworks and the necessity of adequate risk capital in banks. Andersen (2011) pointed out that operational risk factors played a significant role in the financial crisis 2007/2008, claiming that the ignorance of operational risk management in banks resulted in poorly documented loans contributing to erroneous assessment of borrowers' creditworthiness. Warren Buffett (1993) claimed that risk comes from not knowing what you're doing. This supports Andersen et.al. claim that managers of financial institutions should examine thoroughly their products and understand all the different risks related to their business. De Johgh E. and de Jongh D. (2013) explored capital adequacy for operational risk and concluded that guideline for Advanced Measurement Approach for calculating capital allocation should be improved, even though considerable progress has already been made (BCBS, 2011). Cristea, M.-A (2021) in her studies concluded that the basic indicator method was mainly utilized for the assessment of the minimum capital requirement for operational risks in 2018. At the same time during her studies a continuous increase in the percentage of the use of the standardized approach and advanced measurement approach were discovered. Muhtaseb, H. and Eleyan, D. (2021) studies indicate that in the banking sector the most related to operational risk management are the financial-statement analysis, product profitability analysis and total quality management, confirming that monitoring and reporting of findings to the management is essential. Erzurumlu, Y. O. and Avci, G. (2021) provided evidence from Turkey that supported previous statement, that these two factors are the most important in the internal governance of banks: organization of the internal governance mechanisms, meaning structured controls and monitoring, and sufficient reporting to senior-level management in banks that secure that banks' products and processes are transparent for shareholders.

Xu Y., Tan T.F. and Netessine, S. (2021) studied how workload affects banks' operational risk event occurrence. They found out that due to high workload employees are making more standard mistakes, as they

are multitasking, however due to low workload employees tend to make performance-seeking risks. Afterwards they concluded that recruiting flexible personnel can considerably diminish the number of operational risk events by 3.2 %–10 %. This can be achieved by allowing employees to be flexible in their working responsibilities, for example, switching their business lines or changing branches within the same organization on a quarterly basis. Other observations indicate that frequency of operational risk events increased significantly with bank complexity (Chernobai, A., Ozdagli, A., Wang, J. (2021), meaning the activities of banks outside the traditional business of banking, here evidence from U.S. bank holding companies. The authors followed interpretation of term complexity provided by the Bank for International Settlements (BIS) and the Federal Reserve (BCBS, 2014). The results showed that larger complexity increases operational risk not only in banks' nonbanking business lines, but also in their core banking business line. Their experiments are strong by the fact that they are possible to replicate, and their findings are robust to an extensive array of tests. One of the operational risk management challenges is to assess the value of the maximum potential losses. Saputra, M.P.A., Sukono and Chaerani, D (2022) in their studies estimated the maximum potential loss for digital banking transactions using EVaR method. Through the simulation of the loss data for operational risk, they found out the threshold value and got the extreme data value. Afterwards, they used a Kolmogorov–Smirnov test to estimate GPD parameter, generalized Pareto distribution (GPD) method. EVaR was calculated based on portfolio approach to achieve a group of risk values as maximum potential losses. The results of their studies showed that the maximum potential loss is with a 95 % confidence level. Thus, mitigation of operational risk in digital banking is evident. Banks need to pay extra attention to digital banking transactions and reserve funds for potential losses, otherwise banks may face a collapse in unforeseen situations such as a global financial crisis that can happen at any time. Therefore, for risk mitigation activities the potential for maximum loss is an important concern. Much work on the operational risk management methodology has been carried out, yet there are still some critical issues which need to be resolved.

Methodology

The methods used in the research are literature review of empirical studies, comparison, generalization and graphical illustration of statistical information, identification of the main idea of regulatory frameworks and legal documentation. Descriptive statistics is used to analyse the data.

Research results and discussion

The next subsections of this article will present the aim of operational risk in the bank, the purpose of operational risk capital and the key challenges of operational risk management.

Operational risk in banks

In the traditional approach in the financial industry, three fundamental risk categories are defined: credit risk, liquidity risk and market risk. These risks can be divided into six types: systematic or market risk, credit risk, counterparty risk, liquidity risk, operational risk, and legal risk (Santomeo, 1997). In the banking sector, the attention to operational risk has been paid since the late 1990s after such popular cases, when fraud cases led to the bankruptcy of Barings bank and 1 billion USD losses for Daiwas Bank.

Operational risk history commenced in 1998, when the Basel Committee formed a working group that interviewed major banks on the operational risk topic, for instance, internal controls, measurements, procedures, etc. It released a paper on operational risk management based on the survey results, indicating the importance of the development of framework for operational risk. Mr. William J. McDonough, Chairman of the Basle Committee and President of the Federal Reserve Bank of New York, in press releases if the Basle Committee pointed out that “the Basel Committee intends to continue monitoring developments in this area of risk management and encourages banks to share with their supervisors the development of new techniques to identify, measure, manage and control operational risk”. The shortcomings of the survey discussions were grouped in five categories: Management Oversight; Risk Measurement, Monitoring and Management Information Systems; Policies and Procedures; Internal Controls; and View of Possible Role for Supervisors. This raises many questions, e.g., whether financial institutions estimate their operational risk exposure with quantitative measurements.

As pointed out by Froot (2003), operational risk can trigger liquidity and systemic risk in the financial sector. He claimed that this is the consequence of hedging market and credit risk through asset securitization. The gap in operational risk measurement is limited data availability. Other observations indicate that financial institutions are not eager to share sensitive operational loss data. This would also support Jorion’s (2006) conclusion that the source of uncertainty lies inside the organization, and this led to the hypothesis that operational risk is a result of inadequate control inside the organization. Thus, operational risk cannot be ignored in banks, and, according to Zeissler and Metrick (2014), in the “London Whale” case, it points to the shortage of other risk management areas.

In 2001, the Basel Committee on Banking Supervision defined operational risk as a separate category in the Working Paper on the Regulatory Treatment of Operational Risk as follows: “the risk of loss resulting from inadequate or failed internal processes, people and systems or from external events” (Basel II). For internal procedures, banks can adopt their own operational risk definition considering their individual complexity of processes and the severity of operational losses.

Traditionally, risk has been assessed by measuring the *probability of incident* and *consequences*, namely the impact of the incident. In order to identify *consequences*, the authors analysed the data on the operational risk losses from 81 ORX banking members. The data collected from the ORX banking loss reports (Figure 1) indicate that operational loss as a percentage of income has decreased since 2015, probably, banks started to invest more funds in preventive actions and risk mitigation activities, however, the average size of an operational risk event (gross loss) has increased, and it was the largest annual average for the past 4 years in 2020. According to the ORX podcast, the largest losses in 2021 were related to frauds; for instance, Thodex lost 2000 million USD due to internal fraud and ABN AMRO – 575 million USD due to a wrong AML risk classification procedure.

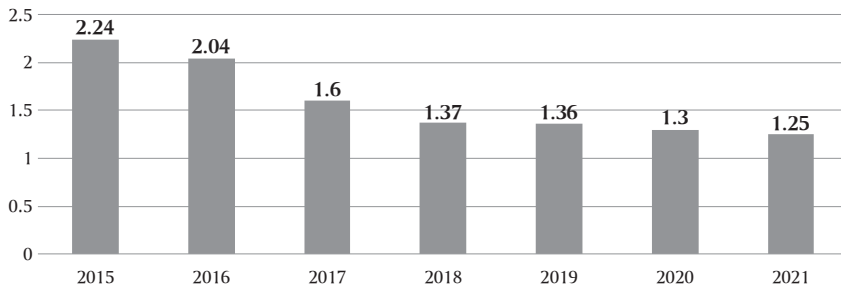


Figure 1. Operational loss to income ratio of ORX international members

Source: Author’s reconstruction of Banking Loss Report 2015–2021 (ORX, 2022)

Most operational losses are due to errors in transaction processing (Harmantzis, 2003). The Figure 2 below demonstrates total gross loss submitted for each event type in 2020 compared to the average across the previous five years. Execution, Delivery & Process management has in general highest losses, 6.5 billion were paid by ORX members only in 2020. Firstly, such losses result from a human error, meaning that everybody can make a mistake everywhere in manual transaction processing. To illustrate this point, let us consider a mistake in the amount or currency made by the employee. To correct the mistake, to return the transaction,

and to pay for currency conversion losses, this cost money for the bank and time for the client. Secondly, the absence or ignorance of properly documented procedures, also called manuals or work instructions, can also lead to the failure of the process. Thirdly, the implementation of control mechanisms in the processes is the key activity for these kinds of mistakes, but it is not always supported by management due to the lack of resources, for example, duality (the four-eyes principle). According to the Annual salary of sustainability analysts in banking operational risk in London in 2018 yearly salary for operational risk manager was 115000 GBP. On the one hand, it takes extra time, employees, and work; on the other hand, these are loss prevention activities for the future. Thus, proper process management is a key to success in operational risk management.

Another topic is external fraud events, according to data gathered from the same source, external fraud is 2 billion EUR higher in 2020 than the average for 2015–2019. Taking into consideration the COVID-19-pandemic, most of the banks were not prepared for this situation and had to improvise how to secure their business in working from home environment. Therefore, cybersecurity and operational risk management for the banks became top priority for the things to re-evaluate. Based on the existing experience, already now banks are reviewing their business continuity plans and crisis management strategies. There was an extreme drop of losses in 2020 in Client, Product & Business Practices. It can be explained again by COVID-19-pandemic, as banks were not focusing on new clients or building new business products, rather than maintaining existing production and rebuilding their ways of working remotely.

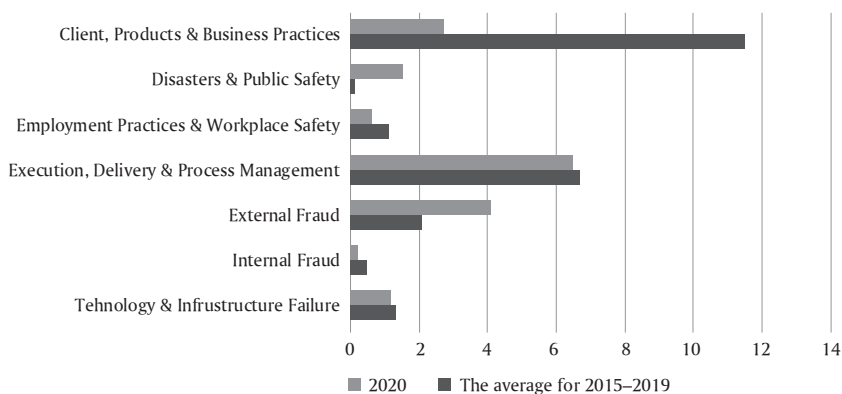


Figure 2. Total gross loss submitted for each event type in 2020 compared to the average across the previous five years (billions, EUR)

Source: Author's reconstruction of Banking Loss Report 2015–2020 (ORX, 2022)

Importance of Operational Risk Management in banks

Operational risk management is the practice of establishing and maintaining the internal controls, reducing errors, meaning, to minimize risks and to avoid losses in the future. It is not a new practice; furthermore, it is widely used not only in banking, but also in the financial industry in general. However, if compared to the management of credit and market risk principles, operational risk management is relatively new. Back in the days, banks improved their internal control mechanisms, complemented by the audit function, to manage operational risk. Nowadays, operational risk is managed within business units, and banks have adapted their organizational structures to manage operational risk in a more effective way. Even though business units are responsible for implementing control within their processes, a separate operational risk department of the bank, as the second line of defence, usually supervises control frameworks. Everything that reduces the probability, or the severity of a loss is a risk mitigation activity and thus is a control (Wernz, 2020). When calculating probability, also called frequency, banks need to evaluate historical data of their incidents and predict probability only based on this data. Unfortunately, as it was mentioned in a lot of sources, not all the banks own and maintain such kind of data or lack its accuracy. The next issue is to calculate the severity or impact of the failure in the process. The calculation of the severity helps managers assess the possible business impact in their processes. When the severity rate is high, managers will see which processes or process steps in their departments can lead to major losses and reputational impact as well. To calculate the impact, banks need to evaluate each process, analyse each step in the process, investigate all the deviations in the process, also analyse other risks that can impact operational risk, for example changes in regulations. For example, changes in payment infrastructure regulated by the central bank. In this case, banks need to adapt systems, processes, and educate people.

Figure 3 illustrates data gathered from 72 monthly ORX Top five largest loss events reports. Table 1 shows descriptive statistics of top 5 monthly losses of ORX members from period 2016 till 2021. The authors analysed 360 incidents, that are top 5 monthly for 6 years.

Three biggest losses happened in China, USD 11.9 billion in March 2018, when former Anbang Insurance chairman embezzles CNY 75.25 billion in illegally raised funds and insurance premium income. In February 2016 there was a loss of USD 7.57 billion for Ezubao, China's largest online financing business, where 21 employees have been arrested under accusations of having defrauded approximately 900,000 investors of CNY 50 billion. In April 2016 Zhongjin Capital Management's owner and at least 20 other people have been arrested following allegations that they illegally raised

around CNY 34 billion in a Ponzi-like scheme between July 2012 and January 2016. All these cases are “Internal Theft & Fraud” event types.

The positive skewness 8.70 with a positive excess kurtosis 93,57 is far from normal distribution, meaning that every year there is a month when the number of amounts observed is a lot higher than average. In July 2020 Deutsche Bank was fined USD 150 million for compliance failures over Epstein, FBME and Danske. It happened in Private banking and event type was classified as Improper Business or Market Practices. The drop in 2021, these are Thodex and ABN Ambro bank cases explained in the previous subsection. Also, the higher the standard deviation, the more spread out the data, in this case 898, the smallest top monthly loss was in February 2021 when BNL vaults were accessed by thieves who had stolen around EUR 1 million by disabling alarm system.

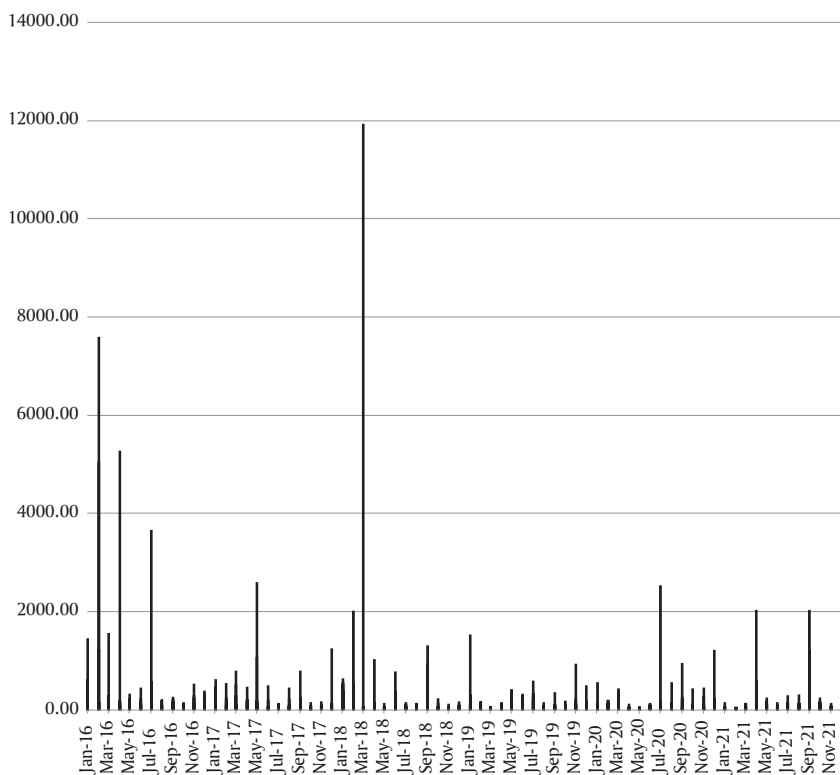


Figure 3. Top 5 monthly losses (millions, USD)

Source: Author's reconstruction of Top five largest loss events Monthly reports 2016–2021 (ORX, 2022)

Table 1. Descriptive statistics of Top 5 monthly losses (millions, USD)

Median	98.65
Mode	100
Standard Deviation	898.4051405
Sample Variance	807131.7965
Kurtosis	93.57083732
Skewness	8.707459764
Range	11898.8
Minimum	1.2
Maximum	11900
Sum	107692.79
Count	360
Confidence Level (95.0 %)	93.11843619

Source: Author’s reconstruction of Top five largest loss events Monthly reports 2016–2021 (ORX, 2022)

The pie chart, Figure 4, shows proportion of losses divided by business line for all 360 incidents, explained above. The underlying trend is obvious, global markets and corporate items events are around 50 % (22.11 % and 27.80 %) from the whole number of losses. From numbers of incidents perspective, the percentage of such events is not so high, global markets are 12 % and corporate items are 3%, meaning that if incident happens it will be quite expensive for the bank. One of the corporate items examples happened in Romania in March 2016, USD 197 million losses, Astra Asigurari’s former CEO has been blamed for causing RON 800 million in damages by illegally lending company money to other firms he owned.

The global market event example is Société Générale incident that happened in Libya in May 2017. Libyan Investment Authority claimed the bank had secured USD 2.1 billion of trades as part of a “fraudulent and corrupt scheme” involving the alleged payment of USD 58.5 million of bribes, and Société Générale paid EUR 963 million to settle a lawsuit. All the cases described are due to improper business, market practices or frauds. According to PwC’s Global Economic Crime and Fraud Survey 2022, economic crime had reached its highest level and remained relatively stable since 2018. PwC claims that 46 % of reported companies has experienced fraud, corruption or other economic crimes in the last year. Barclays bank in their press release are pointing out that during COVID-19-pandemic the “Fraud Triangle” have been present, or three factors that can urge an

employee to commit fraud: new opportunity, strong money motivation and capacity to rationalize their behaviour (Carpenter, 2022). Working from home with a newly adapted security systems or without adequate oversight and control was normal practice in the beginning of COVID-19-pandemic. Management can not see what employees are doing, which systems are using, therefore it is difficult to detect suspicious behaviour. Regarding motivation of money different sources are supporting Barclays in their statement about general financial pressure under crisis.

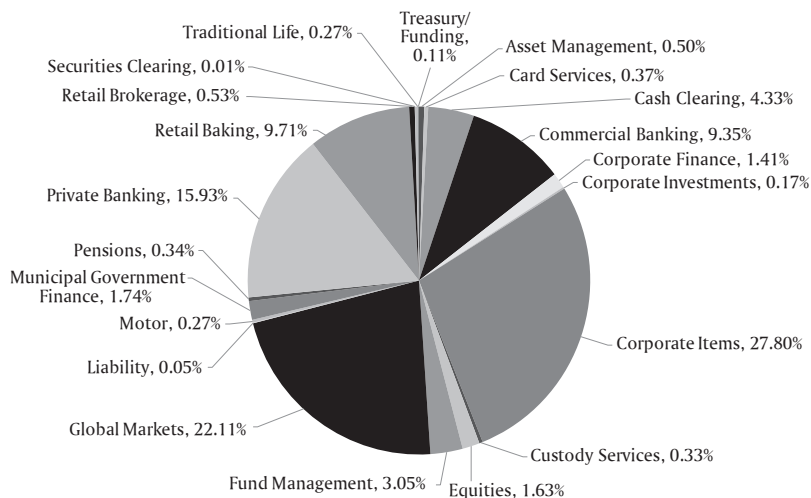


Figure 4. Top 5 monthly losses % by business line

Source: Author's reconstruction of Top five largest loss events Monthly reports from 2016–2021 (ORX, 2022)

With Basel III, operational risk controls are even more substantial, as each loss increases operational risk capital charge utilizing mandatory SMA calculations.

Self-Risk Assessment method is one of the feasible tools used by banks for ascertaining and measuring the operational risk. Self-Risk Assessment is usually driven by operational risk departments within all the units in the banks and includes workshops to identify the gaps of the operational risk environment. Checklists and scorecards are used to translate qualitative assessments into quantitative metrics that give a corresponding ranking of different types of operational risk exposures. The Institute of Operational Risk (2010) described the Risk & Control Self-Assessment (RCSA) as an integral component of a company's overall operational risk management framework that shows a sound system of risk management and offered

the framework for effective internal controls review. They claimed that these techniques and disciplines for estimating the risk can be incredibly subjective and difficult to measure. They argued that the use of RCSA as an integral element that contributes to assessing the results of the operational risk capital charge may be incomplete and concluded that operational risk is an empirical more than a mathematical science. The Risk Management Association (BEICF, 2008) noted that for capital estimation purposes, RCSA results are mostly used for a data loss and scenario analysis. For most of the companies the association recommended using the results to estimate the defined amount for the calculation of capital. The Basel Committee points out that the RCSA tool is mainly used for evaluating capital estimation; however, most of the employees in the companies using this tool believe that the main value of the RCSA is managing operational risk and contributing to assessing accurate results.

The UK FSA's Operational Risk Governance Expert Group (2005) observed essential differences that exist between operational risk and other risk types stating that the direct connection between measurement and management is challenging due to the difficulties in assessing accurate positions of the operational risk that a company faces and how to measure these positions. Six years later they also noted the challenges of creating the right awareness in the organizations towards operational risk culture. These initiatives should be driven by senior management in the organization with the focus of investing in resources in operational risk activities across business units, for example, resources for managing operational risk data and proper operational risk trainings across business units.

Key risk indicators (KRI) are crucial data collection to ensure that all potential pitfalls are considered in the organization. Any changes in KPIs must be reconciled with risk management departments in the banks and managers across all the units in the organization.

Importance of operational risk capital in banks

Froot (2003) was among the first to explain the need of operational risk capital as "collateral on call". To secure the fulfilment of the definition and to manifest the importance of Operational risk in banks, Basel II introduced three operational risk capital measurement methodologies, allowing banks to choose among the Basic Indicator Approach (BIA), the Standardised Approach (SA) and the Advanced Measurement Approach (AMA). Tables 2 and 3 indicate that according to ECB Supervisory Banking Statistics, most operational risk exposure amounts are calculated using Standardised Approach, including G-SIBs, that are global systemically important banks, meaning that banks already preparing for the upcoming changes within Basel review framework.

Table 2. Risk exposures composition by classification

Operational risk exposure amount, Q4 2021. Composition by classification (size), (EUR billions)	Total assets				G-SIBs	Total
	Less than €30 billion	Between than €30 billion	Between €100 billion	More than €200 billion		
Operational risk exposure under BIA	5.04	21.97	10.67	12.76	5.41	55.85
Operational risk exposure under TSA/ASA	7.9	58.96	43.99	145.54	127.66	384.05
Operational risk exposure under AMA	0.82	4.94	16.55	98.03	262.07	382.41
Operational risk exposure amount total	13.76	85.87	71.21	256.33	395.14	822.31

Source: Author's reconstruction, ECB Supervisory Banking Statistics Fourth quarter 2021

Table 3. Risk exposures composition by classification

Operational risk exposure amount, Q1 2022. composition by classification (size), (EUR billions)	Total assets				G-SIBs	Total
	Less than €30 billion	Between than €30 billion	Between €100 billion	More than €200 billion		
Operational risk exposure under BIA	4.22	19.44	10.68	16.03	5.66	56.03
Operational risk exposure under TSA/ASA	7.25	63.76	39.87	151.63	130.55	393.06
Operational risk exposure under AMA	0.78	5.02	19	100.42	257.27	382.49
Operational risk exposure amount total	12.25	88.22	69.55	268.08	393.48	831.58

Source: Author's reconstruction, ECB Supervisory Banking Statistics First quarter 2022

The new Basel III standards introduced in 2017 are gradual changes, where paragraph 644 replaces with 683 of the Basel II framework, prohibiting

the previous operational risk capital measurement methodologies. As a result, all the banks are required to use the Standardised Measurement Approach (SMA), which factors in historical operational risk losses as well as business indicator components (BIC). Essentially, Operational risk capital is ILM (Internal Loss Multiplier) x BIC. No other methodologies are permitted under Basel III as of 2023, as coming in force to the full extend. A Business indicator component (BIC) is a function of income and balance sheet, namely, it is a 3-year average sum of interest, leases, dividend, services, and financial components. ILM (Internal Loss Multiplier) is a factor that is based on a bank's average historical losses for the past 10 years. It means that banks are highly motivated to plan strategically operational risk capital as well as to improve operational risk management in a cost-effective manner to avoid bigger losses, as losses will stay in calculations for 10 years. With Basel III, each loss causes double challenges, as the direct impact on profit/loss and direct impact on future operational risk capital as losses will remain in the history of the bank and, therefore, will increase operational risk capital for many years. The biggest challenge of the changes is the refusal of internal models. The requirements for operational risk capital using internal models are less, therefore, these changes contribute to the increase of operational risk weights in the capital of the bank.

Figure 5 illustrates operational risk capital to income ratio of ORX international members. Average percentage in US is 29 and Europe 13.93, the reason for such difference can be commented that American banks estimations towards operational risk are stricter and they started to work with operational risk management much earlier. ORX members from US are Bank of America, BNY Mellon, State Street and other large companies.

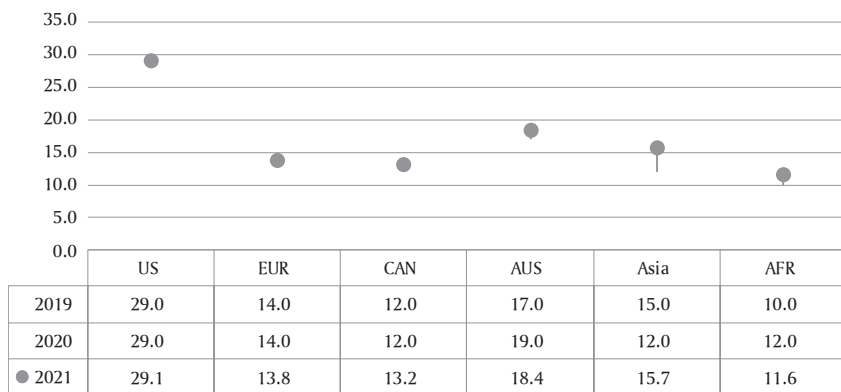


Figure 5. Operational risk capital to income ratio of ORX international members

Source: Author's reconstruction of Banking Loss Report 2015–2021 (ORX, 2022)

Figure 6 shows that in Austria operational risk exposure amount in average from 2015 till 2022 was 11 % of total risk exposure amounts. There is an increase in operational risk amount with low standard deviation 2.08. Maximum value was in September 2017, EUR 34.153 billion were spent for operational risk. The positive skewness 0.56 meaning that every year there is a month when the number of amounts observed is a lot higher than average and distributions with negative excess kurtosis -0.79 means the distribution produces fewer extreme outliers from the normal distribution (Table 4).

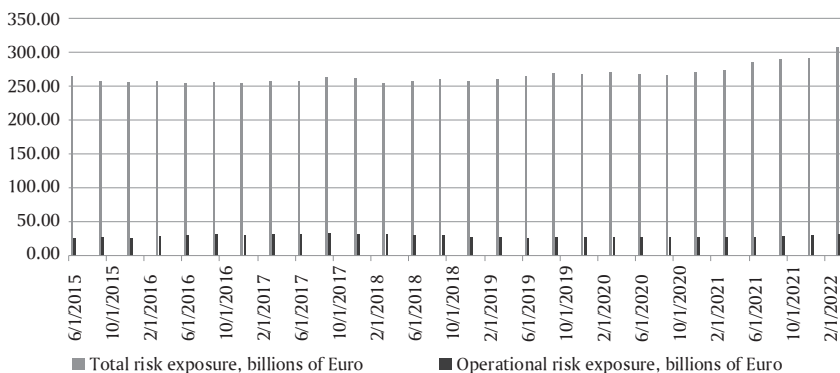


Figure 6. Total risk exposure amount and operational risk exposure amount, Austria, Billions of Euros

Source: Author's reconstruction, Supervisory Banking Statistics, ECB (2015–2022)

Table 4. Descriptive statistics of Operational risk exposure amount, Austria, Billions of Euros

Mean	29.36021481
Standard Error	0.400239376
Median	28.5341
Standard Deviation	2.079704805
Sample Variance	4.325172075
Kurtosis	- 0.79913122
Skewness	0.563583374
Range	7.3281
Minimum	26.8251
Maximum	34.1532
Sum	792.7258

Source: Author's reconstruction, Supervisory Banking Statistics, ECB (2015–2022)

According to Latvian bank statistics, total risk exposure amount for operational risk in Latvia for Q4 2021 was 961,020 thousand of euro. Operational risk capital requirements of total capital requirements average in 2021 was 10.47 %, in Austria it was 11.01. The largest risk exposure amounts for operational risk Latvia in 2021 had Swedbank, 298.769 thousand euros and Citadele banka 146,960 thousand euros quarterly.

Conclusions

This article has argued for the challenges within operational risk management in banks related to the regulatory changes in operational risk capital. Several findings have emerged as a result of the study.

First, this study has identified that with Basel III each loss causes double challenges, as the direct impact on profit/loss and also on future operational risk capital, as losses will remain in the history of the bank for many years.

The second finding has showed that even though loss percentage of income is decreasing, banks are still investing more funds in operational risk capital. Also, interesting fact that US banks are investing almost twice more money to operational risk capital than European.

The third finding was related to Top five monthly losses across ORX members. The biggest amounts of losses are related to corporate items events and the positive skewness 8.70 with a positive excess kurtosis 93.57 is far from normal distribution.

Another finding was that most of the banks were not prepared for COVID-19-pandemic and had to review operational risk procedures immediately to secure their business in working from home environment.

The results of this study indicate that an efficient way of operational risk assessment is to set up a framework for regularly monitoring and registering the frequency, severity, and other applicable information on individual loss events.

These findings suggest that identifying and addressing these shortcomings can significantly reduce the potential frequency and/or severity of a loss event immediately.

The research has also shown that an effective controlling process is crucial for successfully managing the operational risk, but at the same time it is expensive. However, a tremendous number of banking transactions can increase several operational errors that can cover higher costs to diminish the consequences.

Much work on the potential of the improvement of operational risk management has been carried out, yet there are still some critical issues which need to be resolved, calculating the severity of the process.

Further research should be carried out to establish a model for calculating severity of the processes. This would be a fruitful area for further work. The study findings are contributing to assessing general gaps of operational risk management and operational risk capital. This article provides comprehensive overview of the topic and will be used for further research within operational risk.

REFERENCES

- BCBS, 2001. Working Paper on the Regulatory Treatment of Operational Risk [online] Available at: Working Paper on the Regulatory Treatment of Operational Risk - Basel Committee (Sep 2001) (bis.org)
- BCBS, 2011. Operational risk: supervisory guidelines for the advanced measurement approaches. Bank for International Settlements. Available at: <http://www.bis.org/publ/bcbs196.pdf>
- BCBS, Basel II: International Convergence of Capital Measurement and Capital Standards: A Revised Framework – Comprehensive Version, June 2006, [online] Available at: www.bis.org/publ/bcbs128.htm
- BCBS, September 1998. Operational Risk Management, [online] Available at: <https://www.bis.org/publ/bcbs42.pdf>
- Business Environment & Internal Control Factors (BEICFs), Industry Position Paper, Risk management Association, December 2008.
- Chernobai, A., Ozdagli, A., Wang, J. Business complexity and risk management: Evidence from operational risk events in U.S. bank holding companies (2021). *Journal of Monetary Economics* 117, 418–440. <https://doi-org.datubazes.lanet.lv/10.1016/j.jmoneco.2020.02.004>
- Cristea, M.-A. Operational risk management in banking activity (2021). *Journal IBIMA Business Review*. DOI: 10.5171/2021.969612, <https://ibimapublishing.com/articles/JEERBE/2021/969612/>
- Diab, A. A.; Metwally, A., Alzakari, A. M., Fazal, A. Banks' concurrent risks during the COVID-19 pandemic: A road map for risk officers and risk management (2022) *Journal of Risk Management in Financial Institutions*. Scopus - Document details - Banks' concurrent risks during the COVID-19 pandemic: A road map for risk officers and risk management (lanet.lv)
- Erzurumlu, Y. O., Avci, G. The Impact of Bank's Internal Governance Mechanism on Operational Loss: Evidence from Turkey. (2021). *Iranian Economic Review*. DOI: 10.22059/ier.2020.76096 https://ier.ut.ac.ir/error_page
- Froot, K. A. Bank Capital and Risk Management: Operational Risks in Context. (2003). Presentation at the Federal Reserve Bank of Boston.
- Hagstrom, R. G. (1994). *The Warren Buffett Way: Investment Strategies of the World's Greatest Investor*. New York: John Wiley & Sons.
- Harmantzis, F. (2003). Operational Risk Management in Financial Services and the New Basel Accord, working paper, Stevens Institute of Technology.

- Jongh E., de Jongh D., de Jongh R., de (2013). A review of operational risk in banks and its role in the financial crisis, Centre for Business Mathematics, and Informatics (BMI), North-West University South African Journal of Economic and Management Sciences.
- Jorion P. *Value at Risk: The New Benchmark for Managing Financial Risk*, 2006, NY, USA.
- Muhtaseb, H., Eleyan, D. The role of management accounting practices in operational risk management: the case of Palestinian commercial banks. (2021). *Journal of Operational Risk*. DOI: 10.21314/JOP.2021.012, <https://www.risk.net/journal-of-operational-risk/7898876/the-role-of-management-accounting-practices-in-operational-risk-management-the-case-of-palestinian-commercial-banks>
- O.R.X. Capital Benchmark 2021 summary report. Available at: <https://members.orx.org/orx-publications/capital-benchmark-2021>
- Public Individual Quarterly Reports by Banks. Latvijas Banka. (2021). Available at: Banku_Publ_cet_4Q_2021_V3.xlsx (live.com)
- PwC's Global Economic Crime and Fraud Survey (2022). Available at: <https://www.pwc.com/gx/en/services/forensics/economic-crime-survey.html>
- Santomero, A. (1997). Commercial Bank Risk Management: An Analysis of the Process, *Journal of Financial Services Research*, 12 (2/3), 83–115. Kluwer Academic Publishers.
- Saputra, M. P. A., Sukono, Chaerani, D., Estimation of Maximum Potential Losses for Digital Banking Transaction Risks Using the Extreme Value-at-Risks Method (2022). *Journal Risks*, 10 (1), 10. <https://doi.org/10.3390/risks10010010>
- Sound Practice Guidance - Risk Control Self-Assessment, Institute of Operational Risk, 2010.
- Supervisory Banking Statistics. ECB, 2021. Available at: <Supervisory Banking Statistics - Fourth quarter 2021> (europa.eu).
- The growing threat of internal fraud. Barclays Bank. Available at: <https://www.barclayscorporate.com/insights/fraud-protection/internal-fraud/>, 2022.
- UK Financial Services Authority Operational Risk Corporate Governance Expert Group, 2005, The Use Test. Available at http://www.fsa.gov.uk/pubs/international/orsg_use_test.pdf and 2011 <https://www.fca.org.uk/publication/guidance-consultation/guidance11.pdf>
- Wernz J. *Bank Management and Control. Strategy, Pricing, Capital and Risk Management*, 2nd ed. Switzerland, 2020.
- Xu Y., Tan T. F., Netessine, S. The Impact of Workload on Operational Risk: Evidence from a Commercial Bank. (2021). *Journal Management Science*, 68 (4), 2668–2693.
- Zeissler, A. G., Metrick A. JP Morgan chase London whale Z: Yale Program on Financial Stability Case Study, 2014. Available at: <https://library.net/document/z3mnw19y-jpmorgan-chase-london-whale-z-background-overview.html>