EGE SCHOLAR JOURNAL

EGE SCHOLAR JOURNAL

Ege Scholar Journal, Year: 2025, Volume: 2, Issue: 2, Pages : 116-123 ***Research Article***

DOI: 10.5281/zenodo.18525416

Publication Date: 30.05.2025

Fatmir Xheladini[1]

1. *University of Tetovo, Str. Ilinden, nn., 1200 Tetova, North Macedonia Email: fatmir.xheladini-ut@unite.edu.mk; ORCID: 0009-0001-1937-9829*

Operational Risk in Banks: Governance, Quantification Models, and Stress Testing under the Basel SMA

Abstract

Operational risk has become a dominant determinant of banking resilience as digitalisation, outsourcing, and interconnected infrastructures increase exposure to ICT outages, cyber incidents, and third-party disruptions. Although the Basel Committee's Standardised Measurement Approach (SMA) enhances comparability of regulatory outcomes, banks still require decision-useful internal measurement supported by disciplined loss-data pipelines, scenario analysis, and strong governance. This study develops an end-to-end operational risk quantification and stress-testing workflow aligned with SMA logic, covering taxonomy and RCSA, loss data validation and lineage, frequency–severity analytics, scenario design, and translation into an SMA-style management capital proxy. Using a structured quarterly dataset, results show that capital pressure increases when loss frequency rises or severity shifts upward, and that cyber and third-party stress scenarios generate disproportionate impacts relative to baseline conditions. The paper provides a board-level reporting template, model-governance controls, and a present–future comparison illustrating how control improvements can reduce capital pressure and concentration risk while strengthening operational resilience.

Keywords: operational risk; Basel III; Standardised Measurement Approach; stress testing; loss data; risk governance; operational resilience

How to cite: Xheladini F. (2025). Operational Risk in Banks: Governance, Quantification Models, and Stress Testing under the Basel SMA. *Ege Scholar Journal, 2*(2), 116-123

1. Introduction

Operational risk—losses arising from inadequate or failed internal processes, people, systems, or external events—has long been recognised as a material risk class in banking. However, its drivers have shifted in recent years. Digital transformation, expanded remote and API-based service delivery, and reliance on outsourced and cloud service providers have increased exposure to ICT failures, cyber incidents, and third-party disruptions. Supervisory expectations consequently emphasise operational resilience: banks' capability to prevent, adapt to, respond to, recover from, and learn from disruptive operational events while continuing critical services.The Basel Committee's reforms, consolidated in Basel III finalisation, replaced internal model approaches for operational risk with the Standardised Measurement Approach (SMA) to reduce unwarranted variability and improve comparability. Yet SMA is not a substitute for robust internal risk management. Banks still need credible taxonomies, high-quality internal loss data, scenario analysis that captures tail risks, and governance capable of demonstrating control effectiveness and auditability.This paper proposes a practical framework that integrates governance and quantification into a single workflow. It focuses on translating frequency–severity analytics and stress scenarios into an SMA-style management capital proxy suitable for risk appetite monitoring, remediation prioritisation, and operational resilience reporting.

2. Materials and Methods

2.1 Research design

A design-science approach is applied: we specify a reproducible operational risk analytics pipeline and demonstrate it with a structured quarterly dataset. The objective is not to replicate the full regulatory SMA computation, but to provide an auditable management proxy that preserves SMA's intuition—capital needs should reflect operational loss experience and control weaknesses.

2.2 Governance and operating model

The framework assigns roles across three lines of defence. The first line owns processes and controls and reports incidents. The second line defines taxonomy, runs RCSA and KRI processes, validates loss data and maintains scenario libraries. The third line independently tests design and operating effectiveness, including model governance, change control, and evidence trails. A board risk committee receives quarterly dashboards integrating losses, KRIs, scenario results, and remediation status.

2.3 Data and definitions

The dataset (Table 1) contains quarterly operational loss event frequency (count), average loss severity (EUR thousands), and an SMA-style capital proxy (EUR millions). In production, the same pipeline is implemented using a central loss database with mandatory metadata fields (event type, business line, root cause, recoveries, and third-party attribution) and validation checks (duplication controls, materiality thresholds, and reconciliation to general ledger accounts).

2.4 Analytics and stress testing

Baseline analytics compute descriptive statistics and correlations. For explanatory purposes, a simple linear proxy links frequency and severity to the capital proxy (not intended for regulatory use). Stress testing uses calibrated shocks: (i) cyber outage stress (higher frequency and severity); (ii) third-party failure stress (moderate frequency, higher severity due to concentration); and (iii) control-improvement case representing strengthened preventive and detective controls.

2.5 Present–future comparison

To operationalise forward-looking decision support, quarters 13–16 are projected under a baseline continuation and a control-improvement pathway, producing comparative capital-proxy trajectories (Figure 4). These projections are scenario illustrations, not forecasts.

3. Results

Table 1 reports the quarterly dataset. Summary statistics (Table 2) indicate mean quarterly frequency of 4.00 events (SD 2.52) and mean severity of 130.7 EURk. The SMA-style capital proxy averages 44.57 EURm. Correlation results (Table 3) indicate that capital pressure is positively associated with both frequency and severity, consistent with a frequency–severity formation view of operational losses. Figure 1 visualises the co-movement of the series (normalized). Figure 3 and Table 4 present stress scenario impacts: cyber and third-party disruptions increase the capital proxy relative to baseline, while control improvements reduce it. Figure 4 provides a present–future comparison showing sustained capital proxy reduction under improved controls.

Table 1. Structured dataset used in this study (quarterly).

Quarter	LossEventFrequency	AvgLossSeverity_EURk	SMA_OpRiskCapital_EURm
1	4	173.9	47.37
2	3	99.3	41.82
3	8	106.8	46.17
4	2	159.0	43.03
5	2	93.0	41.80
6	2	109.2	40.60
7	5	132.9	46.35
8	3	131.4	45.45
9	6	134.8	45.69
10	9	129.3	48.12
11	3	153.6	44.70
12	1	145.4	43.73

Figure 1. Co-movement of operational loss frequency, severity, and SMA-style capital proxy (normalized).

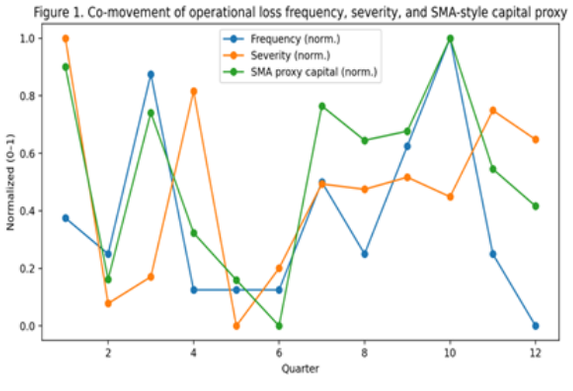


Figure 2. Illustrative proxy diagnostic (fitted vs observed).

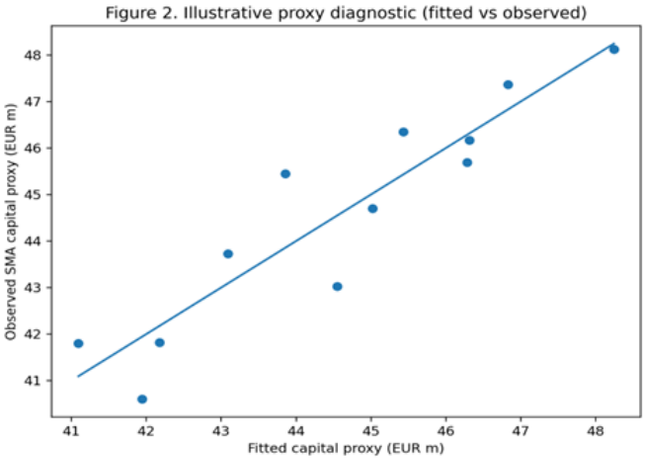


Figure 3. Stress scenarios and control improvement: SMA-style capital proxy impact.

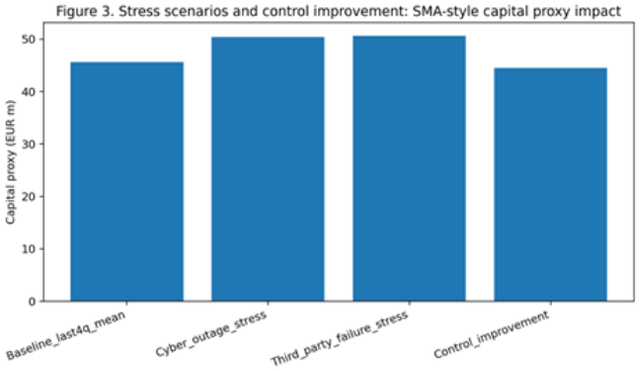
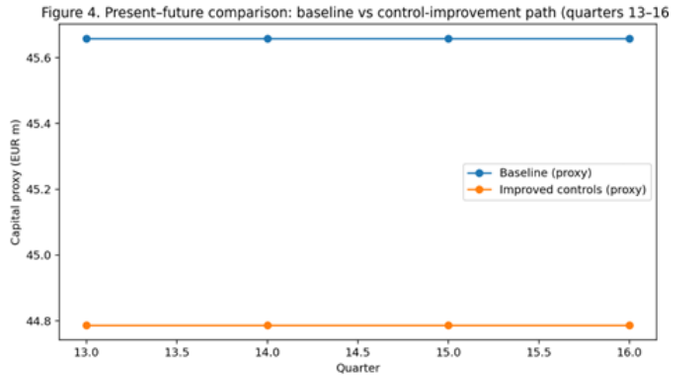


Figure 4. Present–future comparison: baseline vs control-improvement path (quarters 13–16).



4. Discussion

The results have three governance-relevant implications. First, SMA comparability does not replace internal measurement. Management value depends on explaining why capital pressure changes and mapping those drivers to controllable actions. Frequency increases often indicate process breakdowns, control fatigue, or emerging threats (e.g., new fraud vectors), while severity shifts may signal concentration risk, contractual exposure, or weak recovery planning.Second, stress testing should be anchored in operational resilience for critical services and material third-party dependencies. Cyber and third-party scenarios frequently exhibit tail behaviour because disruptions propagate through payment rails, channels, and outsourced platforms. Banks should integrate scenario outputs with KRIs (availability, patch latency, privileged access metrics, vendor SLA breaches) and ensure evidence-grade incident post-mortems.Third, model governance is

essential even for management proxies. Banks should maintain documentation of definitions, data lineage, validation checks, parameter governance, back-testing against realised events, and change control. Boards should receive concise dashboards linking loss experience, top KRIs and thresholds, scenario impacts, remediation progress, and residual risk versus appetite.

5. Conclusions

This paper develops an implementable framework for operational risk governance, quantification, and stress testing consistent with SMA logic. The empirical illustration shows that combined movements in loss frequency and severity influence capital proxy outcomes, and that cyber and third-party disruption scenarios can materially increase capital pressure. Embedding these analytics into enterprise risk management supports prioritisation of control investments, operational resilience testing, and board reporting aligned with supervisory expectations. Future work should extend the framework using event-type granularity, explicit recoveries, and third-party concentration analytics based on service mapping.

6. Patents

Not applicable.

Supplementary Materials

Underlying CSV tables and figure files are provided; computational steps can be shared upon request.

Author Contributions

Conceptualization, F.X.; methodology, F.X.; formal analysis, F.X.; writing—original draft preparation, F.X.; writing—review and editing, F.X.; visualization, F.X.; supervision, F.X.

Funding

This research received no external funding.

Institutional Review Board Statement

Not applicable.

Informed Consent Statement

Not applicable.

Acknowledgments

The author acknowledges institutional support and peer feedback received during manuscript preparation.

Conflicts of Interest

The author declares no conflicts of interest.

Appendix A

Robustness checks: alternative severity measures (median, 95th percentile), event-type stratification, tail fitting for large losses, and sensitivity to data truncation thresholds.

Appendix B

Data dictionary: LossEventFrequency = count of validated internal loss events per quarter. AvgLossSeverity_EURk = average gross loss per event (EUR thousands). SMA_OpRiskCapital_EURm = management capital proxy aligned to SMA logic (EUR millions).

References

1. Basel Committee on Banking Supervision. (2003). *Sound practices for the management and supervision of operational risk*. Bank for International Settlements.
2. Basel Committee on Banking Supervision. (2011). *Principles for the sound management of operational risk*. Bank for International Settlements. Bank for International Settlements
3. Basel Committee on Banking Supervision. (2016). *Standardised Measurement Approach for operational risk* (Consultative document). Bank for International Settlements. Bank for International Settlements
4. Basel Committee on Banking Supervision. (2017). *Basel III: Finalising post-crisis reforms* (BCBS 424). Bank for International Settlements. Bank for International Settlements
5. Basel Committee on Banking Supervision. (2021). *Principles for operational resilience*. Bank for International Settlements. Bank for International Settlements
6. European Banking Authority. (2019). *Guidelines on ICT and security risk management (EBA/GL/2019/04).* European Banking Authority. European Banking Authority+1
7. European Banking Authority. (2019). *Guidelines on outsourcing arrangements (EBA/GL/2019/02).* European Banking Authority. European Banking Authority
8. European Parliament and Council of the European Union. (2022). *Regulation (EU) 2022/2554 of 14 December 2022 on digital operational resilience for the financial sector (DORA).* Official Journal of the European Union, L 333, 27.12.2022, 1–79. EUR-Lex+1
9. National Institute of Standards and Technology. (2024). *The NIST Cybersecurity Framework (CSF) 2.0* (NIST CSWP 29). U.S. Department of Commerce. NIST Publications+1
10. Committee of Sponsoring Organizations of the Treadway Commission. (2017). *Enterprise risk management: Integrating with strategy and performance* (Executive summary). COSO. The IIA Sweden+1
11. International Organization for Standardization. (2018). *ISO 31000:2018 Risk management—Guidelines*. ISO. ISO
12. International Organization for Standardization. (2019). *ISO 22301:2019 Security and resilience—Business continuity management systems—Requirements*. ISO. ISO
13. Chernobai, A., Jorion, P., & Yu, F. (2011). The determinants of operational risk in U.S. financial institutions. *Journal of Financial and Quantitative Analysis, 46*(6), 1683–1725.
14. Cope, E. W., Piche, M., & Walter, J. S. (2012). Operational loss forecasting: A univariate time series approach. *Journal of Operational Risk, 7*(3), 3–33.
15. Cruz, M. G. (2002). *Modeling, measuring and hedging operational risk*. Wiley.

16. Cummins, J. D., Lewis, C. M., & Wei, R. (2006). The market value impact of operational risk events. *Journal of Banking & Finance, 30*(10), 2605–2634.

17. de Fontnouvelle, P., DeJesus-Rueff, V., Jordan, J. S., & Rosengren, E. S. (2006). Capital and risk: New evidence on implications of large operational losses. *Journal of Money, Credit and Banking, 38*(7), 1819–1846.

18. Dutta, K., & Perry, J. (2007). A tale of tails: An empirical analysis of loss distribution models for estimating operational risk capital. *Federal Reserve Bank of Boston Working Paper*.

19. Frachot, A., Georges, P., & Roncalli, T. (2001). Loss distribution approach for operational risk. *Working paper*.

20. Jorion, P. (2007). *Value at risk: The new benchmark for managing financial risk* (3rd ed.). McGraw-Hill.

21. McNeil, A. J., Frey, R., & Embrechts, P. (2015). *Quantitative risk management: Concepts, techniques and tools* (2nd ed.). Princeton University Press.

22. Power, M. (2005). The invention of operational risk. *Review of International Political Economy, 12*(4), 577–599.

23. Shevchenko, P. V. (2011). *Modelling operational risk using Bayesian inference*. Springer.

24. Taleb, N. N. (2007). *The black swan: The impact of the highly improbable*. Random House.

25. Yamai, Y., & Yoshiba, T. (2005). Value-at-risk versus expected shortfall: A practical perspective. *Journal of Banking & Finance, 29*(4), 997–1015.

26. Basel Committee on Banking Supervision. (2006). *International Convergence of Capital Measurement and Capital Standards: A Revised Framework—Comprehensive Version* (Basel II). Bank for International Settlements.

27. Basel Committee on Banking Supervision. (2011). *Basel III: A global regulatory framework for more resilient banks and banking systems* (Revised version). Bank for International Settlements.

28. European Banking Authority. (2024). *EBA amends its Guidelines on ICT and security risk management measures in the context of DORA application* (Press release). European Banking Authority. European Banking Authority

29. Financial Stability Board. (2021). *Principles for operational resilience* (Compendium of Standards entry). Financial Stability Board. Financial Stability Board

30. Daci, E., & Rexhepi, B. R. (2024). The role of management in microfinance institutions in Kosovo: Case study Dukagjini region. *Quality – Access to Success, 25*(202). https://doi.org/10.47750/qas/25.202.22 ORCID

31. Rexhepi, B. R., Murtezaj, I. M., Xhaferi, B. S., Raimi, N., Xhafa, H., & Xhaferi, S. (2024). The cost calculation method based on activity is known as the activity-based costing (ABC) method. *International Journal of Religion*. https://doi.org/10.61707/r9xmrs04 ORCID+1

32. Rexhepi, B. R., Mustafa, L., Berisha, B. I., Vranovci, S. H., & Sadiku, M. K. (2024). Creating a factoring service specifically designed for small and medium enterprises at Pro Credit Bank in Kosovo. *International Journal of Religion*. https://doi.org/10.61707/tc834x95 ORCID+1

33. Rexhepi, B. R. (2024). Investment decisions related to the allocation of capital. *Kuey (journal record as listed in ORCID).* ORCID+1

34. Rexhepi, B. R., & Daci, E. (2024). Analysis of the effectiveness of freelance exchanges and their demand among corporate customers in the context of tax regulation. *Scientific Bulletin of Mukachevo State University Series Economics* (as available via ResearchGate PDF). ResearchGate

35. International Organization for Standardization. (2019). *ISO 22301:2019 Security and resilience—Business continuity management systems—Requirements* (Business continuity standard referenced for resilience design). ISO. ISO