

Call for Papers

Special Issue on “Rising Tide of Operational Risks: Management Controls for Better Risk Management”

Guest Editors:

Sergeja Slapničar, the University of Queensland, Australia

Sebastian Oelrich, TUD Dresden University of Technology, Germany

Operational risks, such as cyber risk, pandemics, natural disasters, terrorism, geopolitical uncertainties, a lack of employees' skills, fraud, supply chain risk, and failure of processes and systems are more pervasive than ever before (ECIIA, 2022; World Economic Forum, 2023). They contribute to the increased complexity of the business environment and operations. Not only that operational risks require adequate procedures and management controls, but when materialising, existing management control tools may show limited usefulness. How can management control tools that address such risks be designed and used? Challenges are numerous: Operational risks have been notoriously difficult to measure due to the rarity of events, the novelty of threat types and the scarcity of data (Wahlström, 2006, 2009). Apart from their wide-ranging nature, operational risks differ from other significant risks due to their loss distribution pattern, characterised by a higher frequency of small losses with low impact and a few rare but high-impact losses (black swan events) (Kay & King, 2020; Taleb, 2009). These unique characteristics challenge quantifying, managing, and overseeing operational risks.

Risk management of various operational risks tends to be confined to silos and special, often self-managing teams (security specialists, compliance officers, crisis managers). While some *internal* operational risks, such as fraud or cyber breach, may be managed with boundary and belief systems (codes of conduct, training, organisational culture and transparency) (Bussmann & Niemeczek, 2019; Oelrich, 2021; Posch, 2020), managing the risks coming from *external* disruptions calls for different approaches, such as stress testing, scenario analysis, contingency planning and crisis management (Harrer & Wald, 2016; Kaplan & Mikes, 2012) or, for example, in case of supply chain risks - risk performance target setting, information sharing, supplier support and joint problem solving (Dekker, Sakaguchi & Kawai, 2013).

While recent advances in digital technology allow risk detection to become more effective (Andreassen, 2020; Fähndrich, 2023), a methodological shift is taking place from risk prevention and detection to building resiliency, encompassing response and recovery (Tsen, Ko & Slapničar, 2022). These approaches demand different forms of management control. One aspect is how organisations approach high-level risk management standards and guidelines (e.g., ISO/IEC 3100) with numerous discretions (Jemaa, 2022). Second, operational risk measurement heavily relies on expert judgment, and research is largely lacking on what biases

risk specialists are prone to when estimating highly uncertain events (Montibeller & Winterfeldt, 2015; Thomsen & Skaerbaek, 2018). Third, quantifying operational risks to compare them to other risks causes considerable frustrations and hinders their integration with Enterprise Risk Management (Boehm, Laube, & Riek, 2018; Ittner & Oyon, 2020; Mikes & Kaplan, 2015; Pollmeier, Bongiovanni & Slapničar, 2023;). Fourth, organisations seem to have different approaches to the measurement of operational risks, from pragmatic ones, based on qualitative assessments and narratives to idealist, pursuing quantification with statistical and machine learning approaches (Arena et al., 2010; Mikes, 2009, 2011; Slapničar et al., 2023). It is not well understood which factors affect the adoption of alternative approaches and how effective they are for risk outcomes. Fifth, the scarcity of studies exploring the behavioural aspects of operational risk management further hinders our understanding of how firms design risk-focused control practices to embed risk considerations in employee decision-making (Posch, 2020) and why risk management failures persist (Meyer, Grisar, & Kuhnert, 2011). Last but not least, temporal dynamics play an essential role (Ahrens & Chapman, 2007; Klein & Reilley, 2021): when risks such as a pandemic, major fraud or natural disasters occur, how do organisations use traditional management controls such as attainment of budgets and incentivising employees.

The insufficient research on the intertwining between operational risk management and management control prompted the proposal of this Special Issue. The Guest Editors aim to foster diverse investigation of management controls for operational risk management encompassing various types of risks and theoretical perspectives, utilising a range of methodologies and data—including quantitative, such as surveys, experiments, and archival research, as well as qualitative approaches, including ethnographic work and case studies—and examining different contextual settings.

We are particularly interested in—but not limited to—the following questions and research avenues:

- The role of management control practices in operational risk management (e.g., approaches in identifying business impact of operational risks, scenario analysis, key risk indicators, internal loss data collection and analysis, incentive systems, codes of conduct, corporate culture, contingency planning, prevention systems; measuring likelihood and consequences of operational risks)
- Theories explaining the adoption of a particular management control approach in operational risk management
- Management controls for operational risks in different types of organisations, including SMEs, not-for-profits, or governmental organisations
- The qualitative versus quantitative assessment of operational risks and their implications for management control
- The incorporation or exploitation of behavioural biases in operational risk assessment and management control practice
- Internal and external communication and sensemaking of operational risk (reports)
- The role of risk managers and management accountants in measuring operational risks
- Management controls for operational risks in different cultural and institutional contexts
- The role of traditional management controls in times of crisis (e.g., during a pandemic, during and in the aftermath of a major cyber-attack, fraud, natural disaster, pandemic, etc.)

We encourage studies that deal with issues beyond the well-established area of climate change risks, as the latter receive ample research attention in accounting journals and their regular and special issues (e.g., Christensen et al., 2022; Clarkson et al., 2023).

Journal of Management Control (JoMaC) is an international journal concerned with the formal and informal, information-based routines and procedures managers use to maintain or alter patterns in organizational activities. Particular emphasis is placed on operational and strategic planning and control systems and their processes and techniques. **JoMaC** has a strong reputation as a dedicated academic journal open to high-quality research on all aspects of management control. JoMaC is available via its publisher Springer at more than 8,000 institutions worldwide. The journal has a high download usage, a high impact factor and short review and production cycles. Accepted papers are published online first 20 to 25 days after acceptance.

We kindly invite authors to submit their papers for a double-blind review process using our electronic review system *Editorial Manager*. Please feel free to contact us if you have any further questions.

Language: English

Review: Double-blind review process

Length: 8,000 words excluding abstract, footnotes and references, 1.5-spaced

Deadline: May 31, 2024

Submissions submitted earlier are welcome and will be send out for review shortly after submission also before the deadline.

Submissions via Editorial Manager: <https://www.editorialmanager.com/jmac/>

Guest Editors:

Sergeja Slapničar

Associate Professor in Accounting

The University of Queensland, Australia

s.slapnicar@business.uq.edu.au

Sebastian Oelrich

Post-Doc Research Associate

TUD Dresden University of Technology, Germany

sebastian.oelrich@tu-dresden.de

References:

- Ahrens, T., & Chapman, C. (2007). Management accounting as practice. *Accounting, Organizations and Society*, 32(1-2), 1-27.
- Andreassen, R.I. (2020). Digital technology and changing roles: a management accountant's dream or nightmare?. *Journal of Management Control*, 31, 209–238.
- Arena, M., Arnaboldi, M., & Azzone, G. (2010). The organizational dynamics of Enterprise Risk Management. *Accounting, Organizations and Society*, 35(7), 659-675.
- Boehm, R., Laube, S., & Riek, M. (2018). A fundamental approach to cyber risk analysis. *Variance*, 12(2), 161–185.
- Bussmann, K.-D., & Niemeczek, A. (2019). Compliance through company culture and values: An international study based on the example of corruption prevention. *Journal of Business Ethics*, 157(3), 797-811.
- Christensen, H., Hales, J., O'Dwyer, B., & Peecher, M. (2022). Conference on accounting for sustainability and climate change. *Accounting Organizations and Society*.
- Clarkson, P., Amel-Zadeh, A., Li, Y., Tang, Q., & Gao, S. (2023). Corporate carbon accounting and management for green transition toward carbon neutrality. *British Accounting Review*.
- Dekker, H., Sakaguchi, J., & Kawai, T. (2013). Beyond the contract: Managing risk in supply chain relations. *Management Accounting Research*, 24(2), 122-139.
- European Confederation of Institutes of Internal Auditing (ECIIA) (2022). *Risk in Focus: Hot Topics for Internal Auditors*. Retrieved from <https://www.eciia.eu/wp-content/uploads/2021/09/FINAL-Risk-in-Focus-2022-V11.pdf>. Institute of Internal Auditors, Risk in Focus 2023, available at <https://iia.no/risk-in-focus-2023/>
- Fähndrich, J. (2023). A literature review on the impact of digitalisation on management control. *Journal of Management Control*, 34, 9-65.
- Harrer, J. & Wald, A. (2016). Levers of enterprise security control: A study on the use, measurement and value contribution. *Journal of Management Control*, 27, 7-32.
- ISO/IEC 3100. Risk management: Principles and guidelines. Retrieved from <https://www.iso.org/iso-31000-risk-management.html>
- Ittner, C., & Oyon, D. (2020). Risk ownership, ERM practices, and the role of the finance function. *Journal of Management Accounting Research*, 32(2), 159-182.
- Jemaa, F. (2022). Recoupling work beyond COSO: A longitudinal case study of Enterprise-wide Risk Management. *Critical Perspectives on Accounting*. Online first: <https://doi.org/10.1016/j.aos.2022.101369>
- Kaplan, R.S., & Mikes, A. (2012). Managing risks: a new framework. *Harvard Business Review*, 90(6), 48-60.
- Kay, J., & King, M. (2020). *Radical uncertainty, decision-making beyond the number*. New York: W.W. Norton.
- Klein, V., & Reilly, J. (2021). The temporal dynamics of enterprise risk management. *Critical Perspectives on Accounting*. online first: <https://doi.org/10.1016/j.cpa.2021.102363>
- Meyer, M., Grisar, C., & Kuhnert, F. (2011). The impact of biases on simulation-based risk aggregation: modeling cognitive influences on risk assessment. *Journal of Management Control*, 22, 79-105.
- Mikes, A. (2009). Risk management and calculative cultures. *Management Accounting Research*, 20(1), 18-40.
- Mikes, A. (2011). From counting risk to making risk count: Boundary-work in risk management. *Accounting, Organizations and Society*, 36(4-5), 226-245.
- Mikes, A., & Kaplan, R. S. (2015). When one size doesn't fit all: Evolving directions in the research and practice of enterprise risk management. *Journal of Applied Corporate Finance*, 27(1), 37-40.
- Montibeller, G., & Winterfeldt, D. (2015). Cognitive and motivational biases in decision and risk analysis. *Risk Analysis*, 35(7), 1230–1251.
- Oelrich, S. (2021). Intention without action? Differences between whistleblowing intention and behavior on corruption and fraud. *Business Ethics, the Environment and Responsibility*, 30(3), 447-463.

- Pollmeier, S., Bongiovanni, I., & Slapničar, S. (2023). Designing a financial quantification model for cyber risk: A case study in a bank. *Safety Science*, 159, 106022.
- Posch, A. (2020). Integrating risk into control system design: The complementarity between risk-focused results controls and risk-focused information sharing. *Accounting, Organizations and Society*, 86. Online first: <https://doi.org/10.1016/j.aos.2020.101126>
- Power, M. (2007). *Organized uncertainty: Designing a world of risk management*. Oxford: Oxford University Press.
- Power, M. (2009). The risk management of nothing. *Accounting, Organizations and Society*, 34, 6-7, 849-855.
- Simons, R. (1995). *Levers of Control: How Managers Use Innovative Control Systems to Drive Strategic Renewal*. Boston, Massachusetts: Harvard Business School Press.
- Slapničar, S., Axelsen, M., Bongiovanni, I. & Stockdale, D. (2023). The pathway model to five lines of accountability in cybersecurity governance. Forthcoming in *International Journal of Accounting Information Systems*.
- Taleb, N. N. (2007). *The black swan: The impact of the highly improbable*. New York: Random House.
- Thomsen, T. & Skaerbaek, P. (2018) The performativity of risk management frameworks and technologies: The translation of uncertainties into pure and impure risks. *Accounting, Organizations and Society*, 67, 20-33.
- Tsen, E., Ko, R. K. L., & Slapničar, S. (2022). An exploratory study of organizational cyber resilience, its precursors and outcomes. *Journal of Organizational Computing and Electronic Commerce*, 32 (2), 1-22.
- Wahlström, G. (2006). Worrying but accepting new measurements: the case of Swedish bankers and operational risk. *Critical Perspectives on Accounting*, 17(4), 493-522.
- Wahlström, G. (2009). Risk management versus operational action: Basel II in a Swedish context. *Management Accounting Research*, 20(1), 53-68.
- World Economic Forum (2023). World Economic Forum Global Risk Report. Retrieved from https://www.weforum.org/reports/global-risks-report-2023?gclid=Cj0KCQjwn_OlBhDhARIsAG2y6zPKYQUNIDbOP0P5JOfBSpuqeAPmGXgBWUoMsg9W-NRUiltjKFVvosaAhswEALw_wcB