Risk Management Strategies for the Banking Sector to Cope with the Emerging Challenges

Tomer Kedarya
Doctoral Student, Tomerked@gmail.com

Amir Elalouf
Head of the Technology Management Program, Lecturer, and Researcher, Amir.elalouf@biu.ac.il

Department of Management, Bar-Ilan University, Ramat Gan 5290002, Israel

Abstract

The banking industry is facing unprecedented challenges, including cybersecurity threats, the need for rapid technology upgrades, a high degree of uncertainty, aggressive entry of technology giants into the financial market, and others. Like most traditional sectors, banks are trying to keep up with the pace of change, monitor emerging risks, and adjust their development strategies. The article analyzes the emerging trends for the banking sector globally and, in particular, in the context of Israel. Interviews with representatives of the most influential national banks formed the information basis of the study. Shifts in corporate strategies, requests for new business models and «working with the future» were identified. The results emphasize the importance of an integrated, holistic approach to risk management and may be useful for banks not only in Israel, but also in other countries and regions.

Keywords: innovation strategies; future of banks; transformation; new technologies; financial innovation; risk management; stress testing; foresight; scenario planning

Citation: Kedarya T., Elalouf A. (2023) Risk Management Strategies for the Banking Sector to Cope with the Emerging Challenges. *Foresight and STI Governance*, 17(3), 68–76. DOI: 10.17323/2500-2597.2023.3.68.76

Introduction

Global challenges place new demands on response and technological upgrade strategies in many sectors, including the financial one. Striving for economic stability is becoming a driver for revising risk management approaches, and for enriching them with new content (Braumann et al., 2020; Arshad et al., 2016). The role of the banking industry in the economy remains vital due to increasingly more stringent regulations (Storm, 2018; Sawyer, 2014).[1] The state uses banking mechanisms to achieve economic growth without significant inflationary costs (Alaeddini et al., 2023; Mishi, Tsegaye, 2017). While the financial sector has a high responsibility, it also faces higher risks than other industries (Domański, 2016). Along with the customary problems regarding lending etc., new, difficult to predict ones are emerging and creating network effects throughout the system, such as, e.g., cyberthreats. In this context the need to revise strategies, and apply advanced monitoring and proactive evaluation technologies sharply increases, including stress testing, foresight studies, scenario planning, etc. Classic risk management tools include such indicators as liquidity and capital ratio, growth rates, return on assets, and financial instruments to total assets ratio (Gouiaa et al., 2020). However, this established "arsenal" turned out to be powerless in the face of major shocks of the last two decades (the financial crisis of 2008, the COVID-19 pandemic, etc.), and the need to quickly adapt to emerging advanced technologies. A broad field has appeared for researching the causes, and finding ways to prevent the recurrence of such systemic failures (Maingot et al., 2018; Ker, 2020; Iavicoli et al., 2021).

This turbulent context has affected the Israeli financial system too, making a negative impact on its performance (Lurie, 2019; Demirgüç-Kunt et al., 2021; Bozou, Benchimol, 2023). The increased regulation of the banking sector during the recession following the global financial crisis turned out to be insufficient to promote economic growth (Rosenberg, 2010). Over the next decade national banks have consistently automated their operations, introduced artificial intelligence (AI) tools, and encouraged customers to switch to digital services (Lurie, 2019). Technological development has been accompanied by such inherent features as increased complexity, uncertainty, and disparity.

The paper attempts to provide a systemic overview of the emerging trends affecting the banking sector and of the risk management literature, and analyse preventive practices of responding to emerging challenges using Israeli banks as an example.

Literature Review

The impact of technological trends on the financial sector

The transformation of the banking sector caused by the rapid technological development, and the future shape of the former are being actively discussed at various venues. Over the past 20 years the average number of cash transactions has decreased by more than 45%, and their per hour intensity by almost a third, while the average transaction cost (previously 85 US cents) has increased by 25%. The average number of daily bank closures is forecasted to increase to 10-15.[2]

Technology companies such as Amazon, Google, Uber, Etsy, etc. may become the largest banking services providers by 2025. The solutions they offer significantly improve user experience, speed up the service, and change relevant standards. The line between fintech players and banks is slowly blurring, leaving the latter facing extraordinary challenges including competition in using broadband communications, AI, cloud computing, and other advanced technologies.

Along with technology giants, small start-up providers are also entering the financial services market.[3] New banks specialising in mobile smartphone applications (such as Neon, Revolut, Transferwise, Zak, etc.) offer attractive services at lower prices than the "classic" ones. The high competitiveness of such players in routine operations including currency exchange is due to a convenient user interface which many conventional banks still fail to offer.[4] In turn, apart from access to advanced technologies BigTech companies have the advantage of possessing immense amounts of customer data.[5]

Among the technologies capable of changing the banking industry landscape, AI is usually singled out, applied to generate investment recommendations, compare products, and interact with customers more effectively.[6] Another transformational technology is blockchain, which increases the reliability and transparency of transactions (Sikorski et al., 2017; Thompson, 2017; Shin, 2017; Li et al., 2018; Drasch et al., 2018; Min, 2019). Its best-known application area is cryptocurrencies (Bitcoin, etc.),

[1] In European countries, the list of routine transactions in which the use of cash is prohibited is growing all the time, so intermediaries in the form of official financial institutions are required to complete them (Lazarus,2017).

[2] http://www.foresightfordevelopment.org/featured/banking, accessed on 14.06.2023.

[3] https:// www.bbva.com/en/the-financial-sectors-new-competitive-scenario/, accessed on 14.06.2023.

[4] https://www.handelszeitung.ch/unterne hmen/revolut-zak-und-co-sind-teilweise-gunstiger, accessed on 14.06.2023.

[5] www.moneycab.com/finanz/banken-rechnen-mit-haerterem-wettbewerb-und-neuen-konkurrenten/, accessed on 14.06.2023.

[6] https://www.forbes.com/sites/danielnewman/2019/01/16/top-7-digital-transformation-trends-in-financial-services-for-2019/, accessed on 14.06.2023.

which allow to make transfers directly without using banks as intermediaries (Eagleton, Williams, 2011; Dwyer, 2015; Makhdoom et al., 2019). This technology is still at an early stage of the innovation life cycle, but it's highly likely to become the main banking tool. The amount of funds generated using it is predicted to increase annually by 100% until 2030 (Harris, Wonglimpiyarat, 2019). Such innovations can radically change the global payment system.

Risk management practices

Risk management is key to sustainable and dynamic development (Loan, 2020). There's no universally accepted definition of this concept, but the essence is in monitoring and assessing threats, developing strategies to minimise them and making use of the emerging opportunities (Dubois et al., 2010; Hansika, Amarathunga, 2016). In the banking sector risks are usually classified by the time of their occurrence, duration, the likelihood of realisation, and the costs of preventing or eliminating the consequences. Most often risks are divided into internal (provoked by unethical or unauthorised actions of personnel) and external ones (those due to macroeconomic shifts, political crises, or natural disasters) (Kaplan, Mikes, 2012). A risk management strategy will help the organisation achieve sustainable development if it's based on a correct assessment of the risk, including its nature (financial, operational, technological, legal, reputational), and was developed by the organisation itself (Smith, 2019, Renn, 2004). Improved regulation of the financial sector, and better communication between its participants also make a positive contribution (Hansika, Amarathunga, 2016).

"Conventional" risks in the financial sector are managed on the basis of the so-called Basel Accords. However, they are updated slowly and thus cannot offer relevant tools to respond to emerging challenges. Accordingly, banks are encouraged to develop flexible, adaptive strategies on their own (Pervez et al., 2022). The financial system must be adapted to such technological trends as the proliferation of blockchain technologies using "regulatory sandboxes" (Guo, Liang, 2016). New approaches are also needed to support more sophisticated customer relations, including customer service, consumer value creation, and brand development (Laketa et al., 2015). The above challenges are in many ways related to the transition to environmentally and socially responsible corporate governance (ESG) (Kalfaoglou, 2021).

The shift to online banking is accompanied by an increase in external cyber-attacks which cause significant damage due to the possible blocking of transactions and leakage of confidential information (Rehman, 2021).[7] Researchers note the high potential of information security technologies such as biometric identification, machine learning, big data analysis, and their various combinations (Ghelani et al., 2022). In particular, it is proposed to use data encryption, special authentication procedures, and multi-level verification (Alzoubi et al., 2022).

The most popular threat response tools include staff training and development, compliance with optimal lending restrictions, and diversification of lending (Youssef, 2019). However, in most cases "getting ahead" requires adopting special strategies designed taking into account various specific aspects (Kaplan, Mikes, 2012). Researchers have paid sufficient attention to common methods such as hedging, diversification, internal management, and capital adequacy ratios (Curti et al., 2020; Gallati, 2022). E.g. hedging is based on setting flexible transaction terms and using "umbrella insurance" (Etges et al., 2019). Diversifying investments across regions and industries has become a common approach, which allows to reduce potential losses in one area by generating income in others (Acharya et al., 2017). However, lack of adequate competencies in alternative investment areas can expose the portfolio to other, unexpected risks (Karkowska, 2019). Yet another possible solution is sharing risks with counterparts through insurance and partnership agreements (Nijskens, Wagner, 2011). However, this approach has its limitations because, despite reduced risks for individual players, at the system level they increase.

In addition, there are capital adequacy requirements to cover customer losses in extreme cases and overcome recession effects. To assess the bank's readiness for possible adverse situations, scenario analysis and stress testing are carried out, as a basis for decision-making. In the increasingly complex context, flexibility, proactive preventive policies, and rapid adaptation to emerging technological and other challenges are of critical importance for banks.

A wide variety of threat assessment and neutralisation tools have been accumulated. However, using then individually is ineffective due to the increased rate of social and technological trends' dynamics. Therefore the existing techniques only work in combination, and in certain cases new, radical approaches must be developed to accomplish particular objectives (Stanikzai, Shah, 2021).

Foresight methods, including scenario planning, monitoring weak signals from the external environment, etc. allow to obtain a better understanding of customers' future behaviour, possible changes in legislation and other uncertainties, which provides a sound basis for strategy development (Jafari, Tabatabai, 2017). The uncertainty aspect forces us to re-

[7] Massive data breaches have become a daily reality. The growing vulnerability of today's digital society is evidenced by regularly appearing news about such incidents involving companies such as Equifax, Chipotle, Gmail, Arby's, Verizon, Yahoo, and Uber.

think the planning process, because tracing all possible causal relationships and effects is too difficult.

An analysis of foresight projects provides an idea of the future context. Recognising their growing reliance on technology and big data, banks are exploring opportunities to gain a competitive advantage by applying them (PWC, 2016). To this end internal think tanks are increasingly being established (Baumgartner, Peter, 2022). Artificial intelligence, blockchain, and other technologies already facilitate transactions' scalability. Against this background, bank personnel find themselves in an ambiguous situation: on the one hand, it becomes possible to focus on complex operations more, while on the other, the number of staff is reducing.

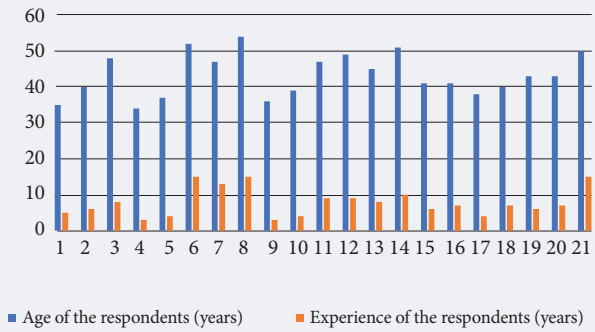
According to various estimates, the future landscape of the financial sector will largely be determined by the strategic course its players take: towards increased competition among themselves, or, on the contrary, strengthening partnerships (or a combination of these approaches). Most banks are still competing to build their own blockchain systems, but for this technology to become widely used, a collaborative cross-industry effort is needed to build an extensive computer and internet infrastructure.[8] Achieving long-term sustainability requires taking a holistic, integrated approach to identifying the emerging drivers today, and correctly interpreting them.

Research Methodology

In line with the abovementioned objective of the study an empirical qualitative approach was chosen, to fully take into account and better understand the various perceptions of the situation and the relevant experience (Creswell et al., 2007; Salloum et al., 2021). Face-to-face semi-structured interviews were conducted with risk managers of major Israeli banks (21 respondents). They were selected to ensure the sample was representative in terms of coverage (national and international banks), specialisation (banks offering mortgages, etc.), location, and other factors. The sample comprised respondents involved in risk management due to their job responsibilities, or those who showed an interest in this topic, had relevant experience and the ability to articulate it. The respondents and the banks have been kept anonymous for confidentiality reasons. Their demographics and work experience details are shown in Figure 1.

To ensure comparability of the results, all respondents were asked the same open-ended questions. Initial assumptions regarding the aspects under consideration were clearly formulated beforehand, to avoid bias in the wording of the questions. During

Figure 1. **Demographics and Job Experiences of the Risk Managers**



Source: authors.

the interviews and between them the focus shifted from broad open topics to more targeted and specific ones (Salloum et al., 2021; Tuffour, 2017). The interviews continued until theoretical saturation was reached, the first signs of which appeared after the fourteenth interview. For greater reliability seven more experts were interviewed, but the "added value" of these conversations turned out to be not significant enough to expand the information basis for the analysis. The minutes and audio recordings were transcribed and converted into electronic text format.

The respondents' characteristics directly related to the object of the study were taken into account. To maintain anonymity, the respondents were assigned codes. The information obtained during the interviews was structured by topic (Table 1), after which a comparative analysis was carried out using ATLAS.ti. The data was checked against the list of initial assumptions to avoid making biased conclusions. In line with the recommendation to use previously published literature as an additional information source (Glaser, 1978), the results of other studies were considered. To further increase the conclusions' reliability, the transcripts were agreed with the respondents. After summarising the interview results the respondents were given the opportunity to provide feedback, which was recorded and made use of. Finally, a summary of all interviews was also made available to the respondents, and adjusted on the basis of their feedback.

Results

The authors' interpretation of the data collected during the interviews served as the basis for identifying the topics for further analysis (Table 1).

Based on mention frequency, the respondents saw data breach-related cyber threats, digital disruptions,

[8] Past experience shows that partnerships between the financial and related industries promote application of financial innovations. Examples include the worldwide network of interbank ATMs Cirrus and the payment systems VISA, MasterCard, UnionPay, JCB, Diners.

Table 1. **Derived Themes and Sub-themes of Study**

Code	Topic	Sub-themes
1	Emerging Challenges and Evolving Risks to the Current Banking Sector	Cybersecurity Threats, technology advancements, economic volatility, regulatory changes, customer expectations
2	Prioritization and Impacts of Evolving Risks and Challenges	Potential impact, regulatory requirements, probability, customer demands, Effects on business models, risk profiles, alignment with organizational objectives, strategic decision-making
3	Difference of Emerging Risks and Challenges from Traditional Risks	Differences in nature, characteristics, impact, mitigation strategies
4	Risk Management Strategies for Emerging Challenges	Risk assessment frameworks, technology solutions, robust internal controls, scenario analysis, compliance measures, stress testing, business continuity planning risk transfer mechanisms
5	Formulation, Implementation, and monitoring of Risk Management Strategies in Banks	Key stakeholders, strategy development, performance monitoring, risk governance frameworks, reporting mechanisms, continuous improvement efforts, alignment with regulatory guidelines.
6	Adapted Risk Management Strategies and their Effectiveness	Identification of strengths, areas of improvement, weaknesses, challenges faced in mitigating emerging risks. success stories.
7	Measurement of the Effectiveness of Employed Risk Management Strategies	Data analysis methods, Key performance indicators (KPIs) reporting frameworks, continuous assessment, benchmarking against industry standards, improvement processes.
8	Collaboration with other Organizations to Tackle Emerging Challenges	Partnerships with other banks, technology firms, industry associations, cross-sector collaborations, academic institutions, regulatory authorities, external consultants, international collaborations.
9	Recommendations and Limitations to Improve Risk Management Strategies	Resource constraints, integration challenges, technological advancements, regulatory complexities, siloed approaches, enhance risk management strategies.

Source: authors.

emerging technologies, customer expectations, economic volatility, regulatory changes, geopolitical uncertainty, market fluctuations, financial crime, and cultural, behavioural, and reputational risks as key challenges for Israeli banks. To detect threats, Israeli banks use careful monitoring, evaluation, audit, partnerships, market research, and feedback analysis (see Table 2 for more).

The banks in Israel rank threats based on their impact, relevance to organisational goals, customer needs, likelihood of realisation, and regulatory requirements. New trends fundamentally affect the Israeli banking sector because they shape customer behaviour, current operations, technology adoption, regulatory environment, risk profiles, business models, and strategic decision making. Approaches based on data analytics, automation, artificial intelligence, and digital currencies (decentralised and cryptocurrencies) are becoming a source of both challenges and opportunities.

The respondents' answers showed that emerging challenges differ from the traditional ones in their nature and effects, and require adapted strategies and special competencies to counter them. They are more dynamic, unpredictable, and complex due to technological development and increased number of cyber-attacks, systemic in nature, and make a cascading effect on the sector in question. The high rate of proliferation, and the lack of statistical estimates for previous periods makes it difficult to identify and quantify such threats. Since they are not covered by a specific regulatory framework, countering them is particularly important for banks' reputation and maintaining customer confidence. This, unlike traditional factors which banks can handle on their own, requires cooperation with other organisations.

To proactively identify and minimise the long-term impact of negative factors, Israeli banks are designing mechanisms for regular monitoring and evaluation. One of the banks has set up a special division responsible for fostering a risk management culture. Its functions include regularly informing the personnel about the nature and consequences of emerging threats, and holding training events to develop relevant competencies.

Cyberthreat monitoring amounts to identifying vulnerabilities using special protocols. Possible response scenarios are developed. The surveyed banks' cooperation with other financial and related organisations, and information sharing help to manage technological risks. Trending provides an information basis for optimising and adjusting management strategies in line with the nature of the challenges. Their effectiveness is evaluated through scenario analysis and stress testing. The risk portfolio can be diversified by distributing assets and investments

Table 2. **Main methods of risk management specified by respondents**

Domain-related risks	Governance methods
Cybersecurity and data privacy	Monitoring, robust risks assessment, vulnerability assessment, audit, staying up dated, penetration testing, data protection regulations
Digital disruption and technological advancement	Monitoring of fintech landscape, assessment of technology risk and collaborations with IT teams
Economic volatility	Scenario analysis, stress testing, and market trend analysis
ESG-related challenges	Collaborations, partnerships, competitive analysis, comparisons of challenges and opportunities

Source: authors, based on interview results.

across regions, lines of business, and sectors. This allows to smooth out the danger zones, balance various impacts, and mitigate the consequences. Taking into account social and environmental factors in developing investment and lending strategies contributes to switching to a green development model.

Risk management strategies are designed by key stakeholders, taking into account the organisation's various outlooks and goals. These strategies are implemented by special divisions responsible for coordinating the tracking of new threats by other bank departments. The collected information is analysed to develop response measures; employees are given appropriate retraining.

Risk management is the subject of open discussions with stakeholders (customers, employees, etc.); the approaches are regularly refined based on the feedback received. The performance is evaluated through independent audit.

The respondents noted that iterative strategy development allows them to proactively identify and minimise the impact of emerging risks on the bank's operations. This process should be regular, based on monitoring, scenario analysis, and stress testing taking into account the characteristics of specific threats to neutralise their consequences. An important role in effective management of, and response to new challenges play partnerships with other banks, industry associations, and fintech start-ups. Cooperation with government agencies contributes to the development of the regulatory framework. The recommendations most frequently suggested by the respondents included increasing investments in infrastructure and analytics tools to better integrate and structure data; stepping up knowledge sharing; strengthening cybersecurity; and implementing inclusive training programmes. Weaknesses mentioned by the respondents included poor integration of knowledge, inability to quickly adapt to new technologies, budgetary constraints, lack of awareness, complex rules and regulations, data privacy vulnerabilities, poor communication, and uncoordinated approaches.

Conclusion

The banking sector is facing various kinds of unprecedented challenges. The most important ones are related to the dissemination of advanced technologies, increased cyberattacks, and pressure from high-tech giants who aim to capture a significant share of the financial market by meeting customer needs better.

Using the Israeli banking system as an example, this paper explores approaches to strategies for countering existing and emerging threats. The information basis was obtained by surveying risk management experts representing Israeli banks. The interview analysis showed that on the whole, the respondents confirmed the priority of the above factors, and applied many of the established management tools including preventive ones.

To improve the effectiveness of the risk management system, the experts first of all recommended to strengthen financial sector organisations' partnership with external stakeholders to share knowledge and experience, increase investment in advanced technologies, regularly monitor the emergence of new threats and opportunities, adapt action plans, and help employees develop relevant competencies.

In general, the study results emphasize the importance of an integrated, holistic approach to security. The existing knowledge on emerging challenges for the banking sector was structured, along with the approaches to managing and ways of neutralising them; the available information was supplemented by an analysis of the situation in Israel. Despite the small sample limitation (21 interviews), the findings may be useful not only for Israeli banks but also for those in other countries and regions, and serve as a guide for further research in this field.

We are grateful to all the reviewers who have shared their valuable comments and suggestions for the research paper. There was no funding required for the completion of the research paper. The authors declare that they have no competing interests.

References

Acharya V.V., Pedersen L.H., Philippon T., Richardson M. (2017) Measuring Systemic Risk. *The Review of Financial Studies*, 30(1), 2–47. https://doi.org/10.1093/rfs/hhw088

Alaeddini M., Madiès P., Reaidy P.J., Dugdale J. (2023) Interbank money market concerns and actors' strategies — A systematic review of 21st century literature. *Journal of Economic Surveys*, 37(2), 573–654. https://doi.org/10.1111/joes.12495

Alzoubi H.M., Ghazal T.M., Hasan M.K., Alketbi A., Kamran R., Al-Dmour N.A., Islam S. (2022) *Cyber Security Threats on Digital Banking.* Paper presented at the 2022 1st International Conference on AI in Cybersecurity (ICAIC), 24-26 May 2022, Victoria, Texas, USA.

Armstrong J., Caldwell G. (2008) Liquidity risk at banks: Trends and lessons learned from the recent turmoil. *Financial System Review*, December issue, 47–52.

Arshad R., Bakar N.A., Othman F. (2016) Board Competencies, Network Ties And Risk Management Disclosure Practices In Non-Profit Organizations. *Journal of Applied Business Research (JABR)*, 32(5), 1319. https://doi.org/10.19030/jabr.v32i5.9761

Baumgartner S., Peter M.K. (2022) Strategic Foresight and Innovation Management: A Comparative Study across International Swiss Banks. *Athens Journal of Business & Economics*, 8(4), 309–328. https://doi.org/10.30958/ajbe.8-4-1 doi=10.30958/ajbe.8-4-1

Bozou C., Benchimol J. (2023) *Desirable Banking Competition and Stability* (Discussion Paper), Jerusalem: Bank of Israel.

Braumann E.C., Grabner I., Posch A. (2020) Tone from the top in risk management: A complementarity perspective on how control systems influence risk awareness. *Accounting, Organizations and Society*, 84, 101128. https://doi.org/10.1016/j.aos.2020.101128

Creswell J.W., Hanson W.E., Clark Plano V.L., Morales A. (2007) Qualitative Research Designs: Selection and Implementation. *The Counseling Psychologist,* 35(2), 236–264. https://doi.org/10.1177/0011000006287390

Curti F., Frame W.S., Mihov A. (2020) Are the Largest Banking Organizations Operationally More Risky? (FRBD Working Paper 2020-2016), Dallas, TX: Federal Reserve Bank of Dallas https://doi.org/10.24149/wp2016

Demirgüç-Kunt A., Pedraza A., Ruiz-Ortega C. (2021) Banking sector performance during the COVID-19 crisis. *Journal of Banking & Finance*, 133, 106305. https://doi.org/10.1016/j.jbankfin.2021.106305

Drasch B.J., Schweizer A., Urbach N. (2018) Integrating the 'troublemakers': A taxonomy for cooperation between banks and fintechs. *Journal of Economics and Business,* 100, 26–42. https://doi.org/10.1016/j.jeconbus.2018.04.002

Dubois É., Heymans P., Mayer N., Matulevičius R. (2010) A Systematic Approach to Define the Domain of Information System Security Risk Management. In: *Intentional Perspectives on Information Systems Engineering* (eds. S. Nurcan, C. Salinesi, C. Souveyet, J. Ralyté), Berlin, Heidelberg: Springer. https://doi.org/10.1007/978-3-642-12544-7_16

Dwyer G.P. (2015) The economics of Bitcoin and similar private digital currencies. *Journal of Financial Stability*, 17, 81–91. https://doi.org/10.1016/j.jfs.2014.11.006

Eagleton C., Williams J. (2011) *Money: A History,* London: The British Museum Press.

Etges A.P.B., de Souza J.S., Kliemann Neto F.J., Felix E.A. (2019) A proposed enterprise risk management model for health organizations. *Journal of Risk Research*, 22(4), 513–531. https://doi.org/10.1080/13669877.2017.1422780

Gallati R.R. (2022) *Risk management and capital adequacy*, New York: McGraw-Hill.

Ghelani D., Hua T.K., Koduru S.K.R. (2022) *Cyber Security Threats, Vulnerabilities, and Security Solutions Models in Banking* (Authorea Preprint, to be appeared in: *American Journal of Computer Science and Technology*). http://dx.doi.org/10.22541/au.166385206.63311335/v1

Glaser B.G. (1978) *Theoretical Sensitivity: Advances in the Methodology of Grounded Theory*, Mill Valley, CA: Sociology Press.

Gouiaa R., Zéghal D., El Aoun M. (2020) An analysis of the relation between enterprise risk management (ERM) information disclosure and traditional risk measures in the US banking sector. *Risk Governance and Control: Financial Markets & Institutions*, 10(1), 61–74. http://dx.doi.org/10.22495/rgcv10i1p5

Grier W.A. (2007) *Credit analysis of financial institutions*, London: Euromoney Books.

Guo Y., Liang C. (2016) Blockchain application and outlook in the banking industry. *Financial Innovation*, 2, 24. https://doi.org/10.1186/s40854-016-0034-9

Hansika W.A.M., Amarathunga P.A.B.H. (2016) Impact of Office Design on Employees' Productivity; A Case Study of Banking Organizations of North Western Province in Sri Lanka (SSRN Paper 2910255). https://doi.org/10.2139/ssrn.2910255

Harris W.L., Wonglimpiyarat J. (2019) Blockchain platform and future bank competition. *Foresight,* 21(6), 625–639. https://doi.org/10.1108/FS-12-2018-0113

Iavicoli S., Boccuni F., Buresti G., Gagliardi D., Persechino B., Valenti A., Rondinone B.M. (2021) Risk assessment at work and prevention strategies on COVID-19 in Italy. *PLOS ONE*, 16(3), e0248874. https://doi.org/10.1371/journal.pone.0248874

Jafari J.M., Tabatabai S.A. (2017) Corporate foresight and its effect on innovation, strategic decision making and organisational performance (case study: Iranian banking industry). *Foresight,* 19(6), 559–579. http://dx.doi.org/10.1108/FS-07-2017-0035

Kalfaoglou F. (2021) ESG risks: A new source of risks for the banking sector. *Bank of Greece Economic Bulletin*, 53, 5. https://doi.org/10.52903/econbull20215305

Kaplan R.S., Mikes A. (2012) Managing risks: A new framework. *Harvard Business Review*, 90(6), 48–60.

Karkowska R. (2019) Model of risk diversification in the banking sector. *Folia Oeconomica Stetinensia*, 19(1), 31-42. http://dx.doi.org/10.2478/foli-2019-0003

Ker A.P. (2020) Risk management in Canada's agricultural sector in light of COVID-19. *Canadian Journal of Agricultural Economics / Revue Canadienne d'agroeconomie*, 68(2), 251–258. https://doi.org/10.1111/cjag.12232

Laketa M., Sanader D., Laketa L., Misic Z. (2015) Customer relationship management: Concept and importance for banking sector. *UTMS Journal of Economics*, 6(2), 241–254.

Lazarus J. (2017) About the universality of a concept: Is there a financialization of daily life in France? *Civitas-Revista de Ciências Sociais,* 17, 26–42. http://dx.doi.org/10.15448/1984-7289.2017.1.25942

Li J., Wu J., Chen L. (2018) Block-secure: Blockchain based scheme for secure P2P cloudstorage. *Information Sciences,* 465, 219–231. https://doi.org/10.1016/j.ins.2018.06.071

Loan L. (2020) The influence of organizational commitment on employees' job performance: The mediating role of job satisfaction. *Management Science Letters*, 10(14), 3307–3312. http://dx.doi.org/10.5267/j.msl.2020.6.007

Lurie L. (2019) New Technologies, Old Problems: Collective Bargaining Agreements and Technology Changes in the Israeli Banking Sector. *Comparative Labor Law & Policy Journal*, 41, 695.

Maingot M., Quon T., Zéghal D. (2018) Risk management by US and Canadian financial firms during the financial crisis. *International Journal of Disclosure and Governance*, 15, 221–234. https://doi.org/10.1057/s41310-018-0049-8

Makhdoom I., Abolhasan M., Abbas H., Ni W. (2019) Blockchain's adoption in IoT: The challenges, and a way forward. *Journal of Network and Computer Applications*, 125(1), 251–279. https://doi.org/10.1016/j.jnca.2018.10.019

Min H. (2019) Blockchain technology for enhancing supply chain resilience. *Business Horizons*, 62(1), 35–45. https://doi.org/10.1016/j.bushor.2018.08.012

Mishi S., Tsegaye A. (2017) *The Role of Banks in Monetary Policy Transmission in South Africa* (ERSA Working Paper 295), Pretoria: National Treasury of South Africa.

Nijskens R., Wagner W. (2011) Credit risk transfer activities and systemic risk: How banks became less risky individually but posed greater risks to the financial system at the same time. *Journal of Banking & Finance*, 35(6), 1391–1398. https://doi.org/10.1016/j.jbankfin.2010.10.001

Pervez A., Mansour N., Bansal R. (2022) A Study on the Implementation of International Banking Standards by BCBS with Special Reference to Basel III Norms in Emerging Economies: Review of Empirical Literature. In: *Artificial Intelligence and COVID Effect on Accounting. Accounting, Finance, Sustainability, Governance &* Fraud: Theory and Application. (eds. B. Alareeni, A. Hamdan) Singapore: Springer, pp. 139–156. https://doi.org/10.1007/978-981-19-1036-4_10

PWC (2016) *Financial services technology 2020 and beyond: Embracing disruption,* London: PricewaterhouseCoopers.

Rehman T. (2021) Cybersecurity for E-Banking and E-Commerce in Pakistan: Emerging Digital Challenges and Opportunities. In: *Handbook of Research on Advancing Cybersecurity for Digital Transformation* (ed. K. Sandhu), Hershey, PA: IGI Global, pp. 163–180. https://doi.org/10.4018/978-1-7998-6975-7.ch009

Renn O. (2004) Systemic risks – A new challenge for risk management: As risk analysis and risk management get increasingly caught up in political debates, a new way of looking at and defining the risks of modern technologies becomes necessary. *EMBO Reports,* 5(S1). https://doi.org/10.1038/sj.embor.7400227

Rosenberg D. (2010) The Israeli Economy: After The Financial Crisis, New Challenges. *Middle East Review of International Affairs*, 14(1), 68–79.

Ruozi R., Ferrari P. (2013) *Liquidity Risk Management in Banks: Economic and Regulatory Issues* (Series: Springer Briefs in Finance), Berlin, Heidelberg: Springer. https://doi.org/10.1007/978-3-642-29581-2_1

Sakal M., Matkovic P., Tumbas P. (2011) Web 2.0 technologies in internal and external communications in the banking sector. *Theory, Methodology, Practice-Review of Business and Management*, 7(2), 87–97.

Salloum S.A., Al-Emran M., Habes M., Alghizzawi M., Ghani M.A., Shaalan K. (2021) What impacts the acceptance of e-learning through social media? An empirical study. In: *Recent Advances in Technology Acceptance Models and Theories. Studies in Systems, Decision and Control* (eds. M. Al-Emran, K. Shaalan), Heidelberg, Dordrecht, London, New York: Springer, pp. 419–431. https://doi.org/10.1007/978-3-030-64987-6_24

Shin J. (2017) *Strategic foresight to generate innovative product concepts*. Paper presented at the XVIII ISPIM Innovation Conference, 16-18 November, Gyeonggi-do, Republic of Korea.

Sikorski J.J., Haughton J., Kraft M. (2017) Blockchain technology in the chemical industry: Machine-to-machine electricity market. *Applied Energy,* 195(1), 234–246. https://doi.org/10.1016/j.apenergy.2017.03.039

Smith A. (2019) The Effect of Leadership Style, Job Satisfaction and Employee-Supervisor Relationship on Job Performance and Organizational Commitment. *Journal of Applied Business Research,* 32(3), 935–945. https://doi.org/10.19030/jabr.v32i3.9667

Stanikzai A.Q., Shah M.A. (2021) *Evaluation of Cyber Security Threats in Banking Systems.* Paper presented at the 2021 IEEE Symposium Series on Computational Intelligence (SSCI), December 5–7, 2021, Orlando, Florida, USA.

Thompson B.S. (2017) Can financial technology innovate benefit distribution in payments forecosystem services and REDD+? *Ecological Economics,* 139, 150–157. https://doi.org/10.1016/j.ecolecon.2017.04.008

Tuffour I. (2017) A Critical Overview of Interpretative Phenomenological Analysis: A Contemporary Qualitative Research Approach. *Journal of Healthcare Communications*, 2(4), 1–5. https://doi.org/10.4172/2472-1654.100093

Youssef A.E. (2019) A Framework for Cloud Security Risk Management based on the Business Objectives of Organizations. *International Journal of Advanced Computer Science and Applications*, 10(12). https://doi.org/10.14569/IJACSA.2019.0101226