# Fintech Banking Risk Taxonomy and Customer Protection: A Systematic Review

**Faraz Ahmed**
College of Business Management,
Institute of Business Management Karachi.
Std_31408@iobm.edu.pk

**Arsalan Hussain**
College of Business Management,
Institute of Business Management, Karachi
arsalan.hussain@iobm.edu.pk

**Arsalan Haneef Malik****
College of Business Management,
Institute of Business Management, Karachi
ORCID: 0000-0001-8940-4850
***Corresponding author*: arsalan.haneef@live.com

**Naeem Uddin Kamran**
College of Business Management,
Institute of Business Management, Karachi
naeem.kamran@iobm.edu.pk

## Abstract

***Purpose***

Digital banks are crucial for the development of a digital financial ecosystem. However, robust risk management is essential to ensure secure services. This includes strong business practices, data protection, and customer education. Legal frameworks and advanced security measures are needed to address transaction risks and build customer trust.

***Methodology***

The current study conducted a systematic literature review on the studies based on different type of types of digital risk.

***Findings***

Findings suggest customer protection and satisfaction are paramount for the future of digital finance. This study's findings also inform digital financial service providers on how to strengthen security and improve customer experience. It also provides valuable insights for future research in this field.

## 1. Introduction

Rapid technical breakthroughs have astounded the world during the last several decades. It has influenced and left an everlasting mark on anything and anything that humans can quantify. The banking sector is one of many examples of technology influencing and changing people's lives and enterprises. The introduction of digital technology into the banking business caused

a paradigm change in the industry, culminating in what is now known as Digital Banking (Sardana & Singhania, 2018).

Authorities are welcoming entrants (fintech and digital banks) as a much-needed injection of competition and innovation into the banking industry as digital banking becomes more widespread throughout the world. To promote digital banking, several authorities have opted to create specific licensing regimes (Choi, 2020). A digital bank is a deposit-taking financial institution that uses a digital-first or digital-only business model to supply its goods and services. Customers are attracted to digital banks because they do not require paper documentation, a physical presence (such as branches, ATMs, or agent point of sale), or manual processing. They also seek to provide an excellent user interface and experience (Choi, 2020).

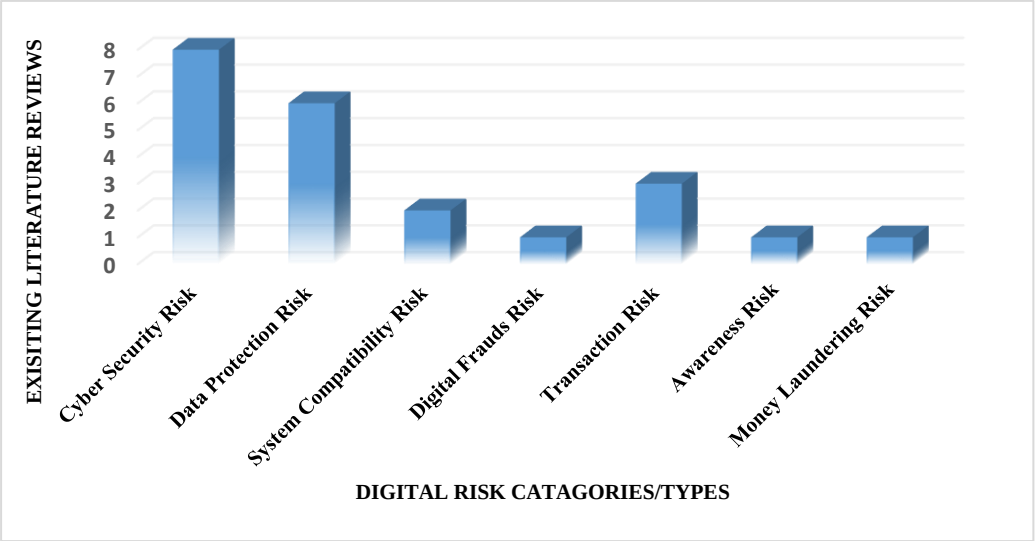
Banks may save money by eliminating queues in banking halls, minimizing manual paperwork and documentation, and maintaining fewer bank branches with digital financial services. It is predicted that banks would be able to reach more clients as a result of digital transformation, which includes the granting of licenses to digital banks and the promotion of financial inclusion through digital financial services (Nathanael & Puspita, 2021).

Digitalization and automation in financial services are major factors that must be addressed. Customers trust banks as a one-stop shop for their requirements because security and client protection are vital to them. However, in this digital banking era, the challenge is how far digital banking can be applied while maintaining the security of consumer transactions and the safety of customers (Kitsios et al., 2021).

There are the issues of cyber security and technology risks (digital risks) related to the protection of customers' data, associated with financial services via fintechs or digital banks (Kitsios et al., 2021). While the digital economy has contributed significantly to productivity growth and the emergence of new forms of banking through digital channels, it has also exposed customers to a variety of risks associated with the use of digital technologies. These risks mainly include data breaches, financial fraud perpetrated using digital technologies, and even cyber-attacks (Kitsios et al., 2021).

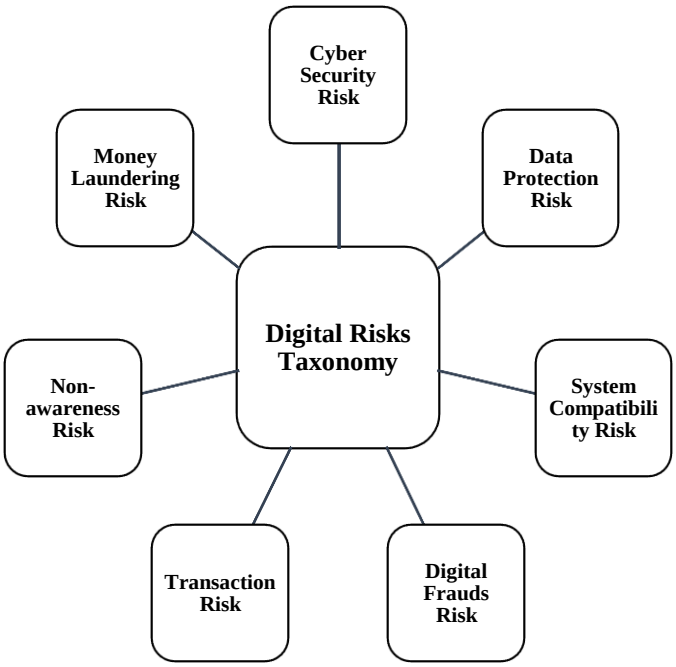
As per the above literature review, financial institutions are exposed to new forms of risks as a result of the rapid rise of fintech innovations and new digital banks. Regulators may confront developing consequences for systemic risk and financial stability. To handle the fundamental new risks posed by digitalized financial ecosystems and the emergence of digital banks, such as "cyber security risk, data protection risk, and digital fraud risk", new tools will almost certainly be required.

The following is a summary of the existing literature on different types of digital risks.




Based on the above analysis, the below taxonomy is devised.

**Fintech Banking Risk Taxonomy:**




### *2.1 Cyber Security Risk*

Based on the above analysis and synthesis of international literature, cyber security risk was found to be one of the top risks associated with digital banks. It has been found that digital banking is increasing the frequency and severity of cyber-attacks (Vives, 2019). As per the literature synthesis, the cyber security risk is a big concern in South Korea, Pakistan, Srilanka, Nigeria, South Africa, Indonesia, and Ukraine. Most trusted financial institutions in these countries are not safe from cyber security and data protection risks. The occurrence of cyber

security cases is on the increasing trend and hackers are taking advantage of internet security violations to damage customer protection.

Customer satisfaction is greatly influenced by their perceptions of cyber security and trust. Customers in the digital financial industry are more advanced, knowledgeable, and demanding. Companies and customers avoid e-commerce operations for several reasons, and cyber security is one of the key reasons (Kumail Abbas Rizvi et al., 2018). Therefore, cyber security is a serious concern when performing financial transactions through digital transaction methods. Moreover, electronic payment systems are currently facing many difficult hindrances posed by the internet (Sahu & Singh, 2018).

To mitigate cyber security risks and to protect the online safety of citizens, various initiatives have been taken by the different international federal & provincial bodies and sectoral regulators such as Electronic Transaction Ordinance, 2002. In this regard, the State Bank of Pakistan (SBP) has also issued different guidelines on cyber security to protect customers from cybercrimes. In Pakistan, Banks are required to enhance their cyber security controls so that cyber-attacks can be responded to on a timely basis. SBP has issued Framework for Risk Management in Outsourcing Arrangements by Financial Institutions (Policy, 2019), instructions on Prevention against cyber-attacks, Regulations for Payment Cards security (Bank, n.d.), regulations on Internet Banking security, and Enterprise Technology Governance & Risk Management Framework for Financial Institutions (Policy, 2017). These all are the initiatives taken by the SBP to enhance the cyber security controls. Banks are also required to develop their internal policy document accompanied by detailed SOPs to safeguard against possible cyber threats. With the help of these initiatives, Banks are successful to mitigate this risk and a low number of successful cyber-attacks have been observed.

### *2.2 Data Protection Risk*

The data protection risk was also found to be one of the key risks associated with digital banks. Customers' data leakage is one of the major challenges in implementing a digital financial ecosystem (Nathanael & Puspita, 2021). The security and safety of dealing via digital banking is a big problem with digital financial services. Identity theft, the loss of personal information, and the abuse of sensitive data are all too common, putting a damper on the use of technology, especially among risk-averse clients.

To mitigate the risk of data protection, General Data Protection Regulation (GDPR) was also introduced. This regulation sets the controls over data access and provides the guideline on the rights and privileges of the use of customers' data. SBP has also issued various guidelines on customer data protection such as Regulation on Data Classification, Guidelines on Outsourcing to Cloud Service Providers, and Enterprise Technology Governance & Risk Management Framework. The main objective of these guidelines is to protect the personally identifiable information (PII) of the customers while doing banking via digital channels. Despite having these detailed regulatory requirements, incidents of data leakage have been found in the industry and this needs to be mitigated by having more stringent policies and roles on data protection.

### *2.3 System compatibility risk*

*System compatibility risk* is also associated with digital financial services. Non-compatibility of the systems leads to software performance issues which ultimately impact customer experience. (Muhtasim et al., 2022) also presented research and found that software performance issue is one of the major elements that influence customer satisfaction level. It has been observed that various operational and system security/compatibility risks arise because of inappropriate and inadequate system architecture and security protocols. To have appropriate system design or technology while designing digital banking products, SBP has issued rules for payment system operators and payment service providers. Under these rules, financial institutions are required to keep their system up to date and keep in line with new technologies. Under SBP regulations, Banks are also required to conduct extensive vulnerability assessments and penetration testing to identify potential weaknesses in their digital banking systems.

### *2.4 Digital fraud risk*

Digital fraud risk is also the key challenge associated with digital banks. It has been found in the literature that a proper digital forensic framework should be implemented to avoid customer protection issues while doing digital banking (Musa, 2019). It has been observed that fraudsters are employing social engineering tactics and fake calls to attempt digital banking fraud. To mitigate this, SBP has designed and deployed additional measures and issued guidelines on fraud risk management. To avoid financial loss, Banks were required to implement detailed verification and dual authentication processes.

### *2.5 Transactional level risks*

Transactional level risks are associated with banking via digital channels. Security of customer transactions shall be also ensured while designing digital banking products and customers must be aware of the risks associated with the digital banks (Noreen et al., 2022). It has been observed that identity verification during online transactions is difficult; therefore, the risk of erroneous transaction processing increased. To mitigate this risk, SBP has implemented different transactional limits during digital transactions so that customer protection can be ensured.

It has been also observed that customers are also not aware of the different types of risks associated with digital banking leading to ***non-awareness risk***. Some governments also implemented Financial Literacy Programs specifically for youth to make awareness about financial resource management within the country (Noreen et al., 2022). To mitigate this risk, SBP has instructed Banks to educate their customers via print, social and electronic media. Customers must be aware of the prevalent digital banking frauds such as SMS and call spoofing. Banks need to educate their customers to not share any confidential information on the phone or by email. Despite these implemented controls, cases of social engineering are on an increasing trend and the main reason behind this is the literacy rate.

The rise of fintech and digital banks' footprints is also accompanied by the dangers of ***money laundering and terrorist funding risks.*** Since, there is no physical presence requirement in

digital banking transactions, therefore; there is a high chance of conducting money laundering transactions (Kumail Abbas Rizvi et al., 2018). To mitigate this risk in the digital banking era, financial regulatory organizations such as the Global Financial Crimes Enforcement Network or Financial Action Task Force (FATF) create laws to protect customers from fraudulent activities and reduce the risk of money laundering terrorist financing. SBP has also issued detailed regulations on Money laundering and as per Regulation 15, Banks should assess money laundering and terrorist financing risks associated with the development of new products, new technologies, and new delivery mechanisms.

Customer satisfaction is greatly influenced by their perceptions of security and trust. Customers in the digital financial industry are more advanced, knowledgeable, and demanding. Companies and customers avoid e-commerce operations for several reasons, and security is one of the key reasons. Therefore, security is a serious concern when performing financial transactions through digital transaction methods. Moreover, electronic payment systems are currently facing many difficult hindrances posed by internet security issues.

**3. How to mitigate Digital Risks**

Banks have a strong interest in delivering services utilizing digital technology. It lowers operational expenses by streamlining back-office operations, reducing errors, and reducing the number of hands required to manage the company. It allows a bank to reduce the number of branches it maintains while delivering more creative and engaging services. This improves the quality, delivery, and efficiency of services, providing digitally enabled banks a competitive advantage. The challenge in setting up a financially inclusive environment is to find out the right balance between supporting financial digitalization and protecting customers. Customers need more assurance in a digital bank that their data and privacy will be respected and safeguarded. This is the only way to promote digitalization when customers feel genuinely safe banking with a digital financial institution.

Regulators have a role to play in promoting the use of financial innovations and digital banks for beneficial purposes. Consumer protection should be prioritized in regulatory regulations and advice, but financial innovation and competition should be encouraged. It is critical to be mindful of the fact that the lack of fintech and digital bank rules may generate substantial uncertainty in the business environment. Following key measures can be taken to mitigate the risks associated with digital banks and to protect customers.

- Electronic know-your-customer requirements (e-KYC). This will allow for totally digital onboarding, with standalone analytics validating consumers' IDs and doing anti-money laundering checks.
- Customers can use e-signature to authenticate most sorts of transactions from afar.
- Third-party assessments from approved assessment bodies.
- Proper encryption mechanisms.
- Proper authentication mechanisms

## 4. Conclusion

Digital banks and digital banking services have evolved and played an important role in the future creation of a digital ecosystem. This can be seen in the significant development of digital banking in various countries around the world, as well as the opportunities that exist. However, such a scenario presents several challenges, particularly in the risk management field. To provide secure digital banking services to the general public, there must be innovative and secure business processes, prudent and sustainable digital banking business practices, adequate risk management policies and procedures, proper governance and IT capability requirements, and guidelines on consumer data protection and the risk of data leakage. This will result in digital banks making a genuine contribution to the development of the digital financial ecosystem.

If there are no laws in place to safeguard customers when they use digital financial services, transaction risk will be significant, leading to customer distrust in the banking sector in general and digital banking in particular. For the digital banking business to develop, better information security management concepts are required. The progress of the digital banking business may be hampered if security considerations are not thoroughly understood. There is also a need to educate and raise awareness among customers about online scams and fraud.

Customer protection and satisfaction will be critical in the future for the growing digital financial industry/digital banks/fintech. To deal with emerging hackers and fraudsters, digital bank security must be advanced. The findings of this study can help digital financial service providers to strengthen system security and focus on critical security factors to improve customer satisfaction and protection when using digital financial services. Furthermore, by taking into account the various factors and variables discussed in this systematic review, this study will help future researchers planning empirical studies in this field.

## 5. References


Bank, S. (n.d.). *Regulations for Payment Card Security PAYMENT SYSTEMS DEPARTMENT*.

Choi, Y. (2020). Digital Banks : Lessons from Korea. *World Bank Group*, *2*. http://hdl.handle.net/10986/34701

Evdokimova, Y., Shinkareva, O., & Bondarenko, A. (2019). *Digital banks: development trends*. *240*(Sicni 2018), 151–153. https://doi.org/10.2991/sicni-18.2019.30

Hornuf, L., Klus, M. F., Lohwasser, T. S., & Schwienbacher, A. (2021). How do banks interact with fintech startups? *Small Business Economics*, *57*(3), 1505–1526. https://doi.org/10.1007/s11187-020-00359-3

Jagtiani, J., & John, K. (2018). Fintech: The Impact on Consumers and Regulatory Responses. *Journal of Economics and Business*, *100*, 1–6. https://doi.org/10.1016/j.jeconbus.2018.11.002

Jayalath, J. A. R. C., & Premaratne, S. C. (2021). Analysis of Digital Transformation challenges to overcome by Banks and Financial Institutions in Sri Lanka. *International Journal of Research Publications*, *84*(1). https://doi.org/10.47119/ijrp100841920212260

JENÍK, I. V. O. (2022). *The Customer Impact of Inclusive Digital Banking*. *January*, 1–9. https://www.cgap.org/sites/default/files/publications/2022_01_Case_Study_TymeBank.pdf

Kitsios, F., Giatsidis, I., & Kamariotou, M. (2021). Digital transformation and strategy in the banking sector: Evaluating the acceptance rate of e-services. *Journal of Open Innovation: Technology, Market, and Complexity*, *7*(3). https://doi.org/10.3390/joitmc7030204

Kumail Abbas Rizvi, S., Naqvi, B., & Tanveer, F. (2018). Is Pakistan Ready to Embrace Fintech Innovation? *The Lahore Journal of Economics*, *23*(2), 151–182. https://doi.org/10.35536/lje.2018.v23.i2.a6

Muhtasim, D. A., Tan, S. Y., Hassan, M. A., Pavel, M. I., & Susmit, S. (2022). Customer Satisfaction with Digital Wallet Services: An Analysis of Security Factors. *International Journal of Advanced Computer Science and Applications*, *13*(1), 195–206. https://doi.org/10.14569/IJACSA.2022.0130124

Musa, A. A. G. and A. (2019). *a Recommended Digital Forensic Readiness Framework for Nigerian Banks*. *09*(June 2020), 28920–28928.

Mutlu-Bayraktar, D., Yılmaz, Ö., & İnan-Kaya, G. (2018). Digital Parenting: Perceptions on Digital Risks. *Kalem Uluslararasi Egitim ve Insan Bilimleri Dergisi*, *14*(1), 137–163. https://doi.org/10.23863/kalem.2018.96

Nathanael, J. J., & Puspita, N. Y. (2021). Jurnal komunikasi hukum. *Jurnal Komunikasi Hukum*, *7*, 387–402.

Naumenkova, S., Mishchenko, S., & Dorofeiev, D. (2019). Digital financial inclusion: Evidence from Ukraine. *Investment Management and Financial Innovations*, *16*(3), 194–205. https://doi.org/10.21511/imfi.16(3).2019.18

Noreen, M., Mia, M. S., Ghazali, Z., & Ahmed, F. (2022). Role of Government Policies to Fintech Adoption and Financial Inclusion: A Study in Pakistan. *Universal Journal of Accounting and Finance*, *10*(1), 37–46. https://doi.org/10.13189/ujaf.2022.100105

Ozili, P. K. (2018). Impact of digital finance on financial inclusion and stability. *Borsa Istanbul Review*, *18*(4), 329–340. https://doi.org/10.1016/j.bir.2017.12.003

Policy, B. (2017). *Enterprise Technology Governance & Risk Management Framework for Financial Institutions*. *05*.

Policy, B. (2019). *Framework for Risk Management in Outsourcing Arrangements by Financial Institutions BANKING POLICY & REGULATIONS DEPARTMENT Framework for Risk Management in Outsourcing Arrangements by Financial Institutions*. *06*.

Sahu, G. P., & Singh, N. K. (2018). *Identifying Critical Success Factor (CSFs) for the Adoption of Digital Payment Systems: A Study of Indian National Banks*. *April*, 61–73. https://doi.org/10.1007/978-3-319-75013-2_6

SSardana, V., & Singhania, S. (2018). *Digital technology in the realm of banking: A review of literature. International Journal of Research in Finance and Management*. *November*, 28–32.

Shin, J. W., Cho, J. Y., & Lee, B. G. (2020). Customer perceptions of Korean digital and traditional banks. *International Journal of Bank Marketing*, *38*(2), 529–547. https://doi.org/10.1108/IJBM-03-2019-0084

Vives, X. (2019). Digital Disruption in Banking. *Annual Review of Financial Economics*, *11*, 243–272. https://doi.org/10.1146/annurev-financial-100719-120854