



## International Journal of Financial Management and Economics

P-ISSN: 2617-9210  
E-ISSN: 2617-9229  
IJFME 2022; 5(1): 149-152  
Received: 04-02-2022  
Accepted: 07-03-2022

**Ramin Abbasov**  
Risk Management  
Department, Rabita Bank  
OJSC, Baku, Azerbaijan

### Managing digital transformation risks in Azerbaijan's banking industry: Best practices and case studies

**Ramin Abbasov**

DOI: <https://doi.org/10.33545/26179210.2022.v5.i1.347>

#### Abstract

The advancement in technology has seen almost every bank in Azerbaijan and the world embrace digital transformation to improve their operations and enhance customer experience. However, the digital transformation in banks has come with a number of risks. Some of these risks include operational disruptions, cyber security threats, and lack of regulatory compliance, among others. To mitigate or prevent these risks, banks must embrace some proven best practices. These best practices include leveraging other technologies like pilot programs, ensuring compliance with regulations and laws, conducting a comprehensive risk assessment, and investing in proper cyber security measures. Besides utilizing best practices in managing digital transformation in banks, banks must learn from other banks that have successfully managed their digital transformation. In Azerbaijan, an example of these banks is the Rabita bank. Having experienced some challenges in digital transformation, these banks have embraced best practices to address these challenges.

**Keywords:** Digital transformation, banking industry, risk management, cybersecurity, best practices, case studies

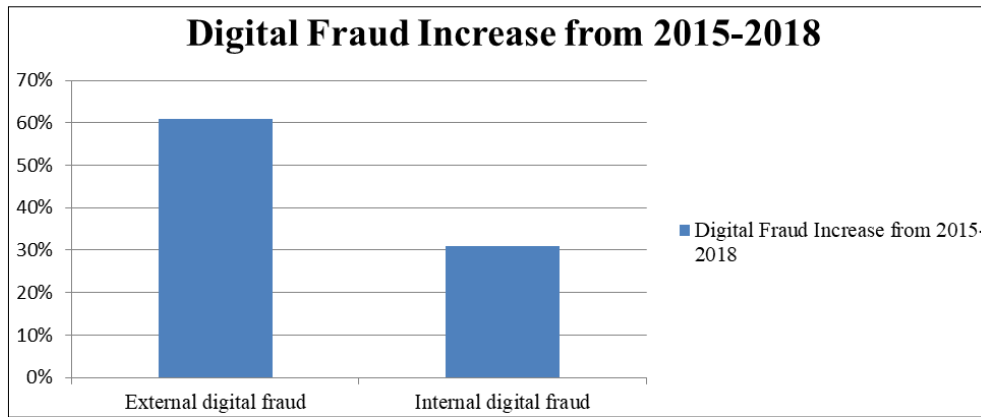
#### Introduction

Technological advancements have impacted almost every sector. As such, the banking sector has not been left behind. The technological advancements have resulted in the banking sector embracing digital transformations. Banks all over the world, especially in Azerbaijan, have embraced digital transformations by leveraging technological features, applications, and platforms to improve their operations and customer experience. In every 30 banks in Azerbaijan, 27 use Internet banking while 25 use mobile banking, showing an over 83 percent embrace of digital transformation in the banking sector (Abbasov and Mamedov, 2019) <sup>[1]</sup>. Additionally, it is projected that Azerbaijan's digital banking market will grow by about 4 percent by 2028, pushing the market volume to about 50 million dollars by 2028 (Abbasov and Mamedov, 2019) <sup>[1]</sup>. However, these digital transformations do not come without some downside. Thus, before one decides to embrace this new wave, Azerbaijan's banking sector must understand the risks that come with these transformations. To assist Azerbaijan's banking industry in effectively managing digital transformation, this paper discusses the risks associated with digital transformation and the best practices for managing digital transformation and includes some case studies as a point of reference.

#### Overview of Digital Transformation Risks

Digital transformation in the banking sector increases the risk of digital fraud. The digitization of the banking industry has seen an increase in digital fraud cases such as authorized push payments, identity theft, and credit card fraud. According to a survey by KPMG International (2019) <sup>[8]</sup>, over 60 percent of the respondents globally stated an increase in external digital fraud volume between 2015 and 2018. At the same time, 31 percent of the respondents reported a rise in internal digital fraud arising from the digitization of the banking sector. Out of these respondents, only 25 percent of them recover their fraud losses (KPMG International, 2019) <sup>[8]</sup>. The low recovery rate of the losses indicates how serious digital fraud is as an impact of digital transformation in banking.

**Corresponding Author:**  
**Ramin Abbasov**  
Risk Management  
Department, Rabita Bank  
OJSC, Baku, Azerbaijan

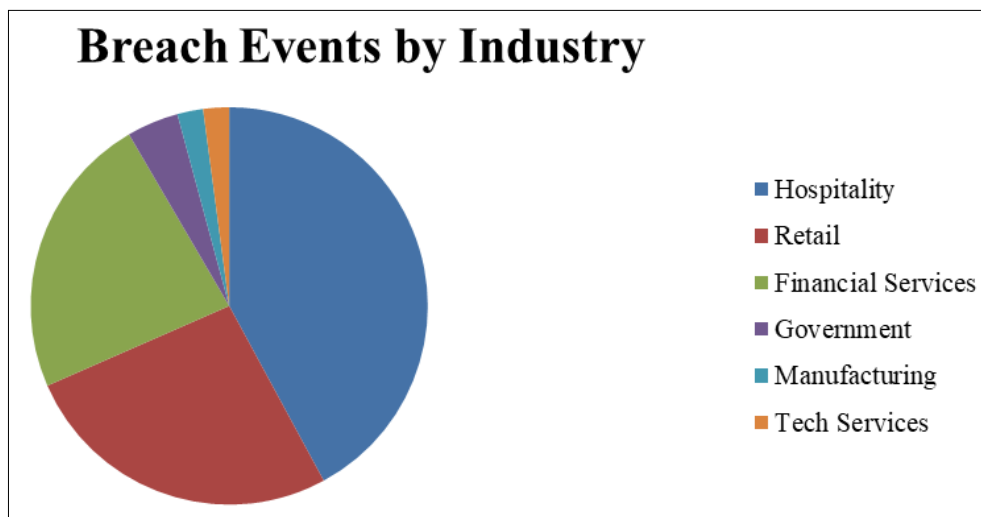


Source: KPMG International, 2019 [8].

Fig 1: Digital Fraud Increase from 2015-2018 in Banks

Another critical digital transformation risk that Azerbaijan’s banking sector should be aware of is the data privacy or data breach issue. With the digital transformation, most of the customers’ confidential data and information is stored electronically. As part of the digital transformation, most of the customers’ confidential data is stored electronically (Betz, 2016) [3]. The electronic storage of data in the banking sector presents various benefits. For instance, electronic storage of customers’ banking data increases the ease of access to the data, reduces storage costs, and

increases efficiency, among other benefits. However, the electronic storage of customers’ data as part of digital transformation exposes the data to the risk of unauthorized access, leading to data breaches. According to a report by Capgemini (2011) [5], the banking industry ranked third in the number of data breaches globally out of the 11 possible industries. Out of the total data breaches recorded in 2010, the banking sector was responsible for 22 percent of the data breaches.



Source: Capgemini, 2011 [5].

Fig 2: Breach Events by Industry

Operational disruption is another digital transformation risk that banks should consider when embracing digital platforms, features, and applications. Operational risks are those risks that arise due to system malfunctions, poor management techniques, staff or employee errors, and other disturbances caused by technology. According to PWC (2021) [10], more than 60 percent of the digital transformation in the banking industry faces delays as a result of integration issues. Furthermore, the report noted that more than 70 percent of the banks embracing digital transformation encounter operational disruptions in their digital transformation initiatives (PWC, 2021) [10]. Therefore, considering the high prevalence of operational risks in the banking sector, Azerbaijan’s banks considering the transformation should be informed.

**Best Practices for Managing Digital Transformation Risks**

Since embracing digital transformation in the banking industry is inevitable, the banking institutions in Azerbaijan must implement best practices to manage the potential risks. Some of these practices include conducting comprehensive risk assessments, investing in proper cyber security measures, implementing data governance procedures and policies, ensuring compliance with regulations, and leveraging emerging technologies to test new technologies before they are implemented.

Comprehensive risk assessment helps banks embracing digital transformations to identify potential risks or threats to the digital transformation and implement the necessary prevention or mitigation measures (Kitsios and Giatsidis, 2021) [7]. For instance, since one of the digital

transformation risks is operational disruptions, a comprehensive risk assessment helps identify any loopholes that may contribute to such risks. According to a survey by Kitsios and Giatsidis (2021) <sup>[7]</sup>, 67 percent of the digital transformation risks in the banking industry are a result of a lack of adequate digital skills among the staff and employees, leading to errors and omissions. These errors and omissions ultimately result in operational disruptions, data privacy issues, and a lack of adherence to regulations. Therefore, a comprehensive risk assessment helps identify such a loophole and address it effectively.

Investing in proper cyber security measures helps address security issues arising from data breaches, thus safeguarding customer data and information in banking institutions. According to Agarwal *et al.* (2021) <sup>[2]</sup>, automating security platforms as a cybersecurity measure in the banking industry reduces the number of data breaches by about 65 percent. Additionally, according to the Financial Services Information Sharing and Analysis Center (2019) <sup>[6]</sup>, implementing proper cyber security measures such as advanced threat intelligence and sharing mechanisms reduces cyberattacks by 40 percent. Thus, considering these facts, it is safe to say that investing in effective and appropriate cybersecurity measures is a proven best practice for managing digital transformation risks in the banking industry.

Another best practice for managing digital transformation risks in the banking industry is ensuring compliance with rules, laws, and regulations. Adhering to regulations and laws prevents the bank from facing risks such as lawsuits, fines, and poor public image. In addition, some regulations provide guidelines on how banks should approach or implement digital transformations. For instance, according to the Ponemon Institute (2018) <sup>[9]</sup> report, organizations that implement and adhere to data protection laws like the General Data Protection Regulation (GDPR) reduce their data breaches by 28 percent. Thus, these regulations are a source of critical information on how banks can avoid some risks, such as cyber security threats.

Before implementing a digital transformation feature or application in a banking institution, the banks must leverage existing technologies to enhance the success of the transformation. Such technologies and inventions, such as pilot programs, allow organizations to test a technology before fully implementing it. According to California Management Review (2018) <sup>[4]</sup>, pilot programs are a useful tool in the implementation of new technology and digital transformation because, firstly, they allow people to learn and adjust their technologies. Through pilot programs, organizations such as banks can introduce technology and learn about its features, ease of integration with the existing systems, and response time (California Management Review, 2018) <sup>[4]</sup>. Since the program is not fully implemented, it allows the organization to adjust it to suit the needs of the organization before its full implementation. Additionally, the pilot programs enable the banks to identify any challenges or changes the program will bring, thus preparing adequately. In pilot programs, the challenges of the technology do not impact the operations of the bank but provide an opportunity to learn more about them and develop prevention or mitigation measures in preparation for a full and seamless implementation at a later date (California Management Review, 2018) <sup>[4]</sup>. Furthermore, pilot programs are advantageous because they are low-cost

compared to the real implementation. With pilot programs, banks can use much cheaper technology and inputs to assess the potential benefits and risks of the technology. If the technology proves disastrous, the organization can abandon it without much implication on its processes.

## Case Studies

### Rabita Bank

One of the banks that have embraced digital transformation in Azerbaijan is the Rabita bank. Formed in 1993, the bank now has 27 branches in various parts of the country, including Guba, Gusar, Sumgayit, Lankaran, Khachmaz, Ganja, Shirvan, Shamkir, Shaki, Shamakhi, Nakhchivan, Kurdamir, Masalli, Aghsu, and Aghjabadi (Rabita Bank, n.d.). To properly position itself in the competitive banking industry, Rabita Bank has embraced digital transformation in various operations and activities. Some of these digital transformations include mobile banking via the mobile application, internet banking, and e-commerce.

The bank conducts internet banking through the AniPay application. Anipay is a mobile application that allows customers to instantly pay for services and products (Rabita Bank, n.d.). Through this system, customers can easily send and receive funds through Internet banking. The instant payment system of AniPay allows customers to transact anywhere and at any time. In terms of e-commerce, the bank has a contactless Point of Service (POS) terminal service referred to as "Verifone X990" that accepts cashless payments. Verifone x990 comes as a thin and light portable smart device with a touch screen that incorporates the latest Android operating system (Rabita Bank, n.d.).

Like other banks that have embraced digital transformations, Rabita Bank has faced various digital risks. These risks include phishing, credit card fraud, and data theft.

To address these risks, the bank implemented various best practices. Firstly, the bank educates its customers about some of these risks and how to avoid them. For example, on the bank's website, there is a security section that describes such risks as phishing. According to Rabita Bank (n.d.), one way to avoid risks such as phishing is by suspecting every website and treating it as a potential security risk. Additionally, customers are advised to inquire from reliable sources about any sites that request them to enter bank account details or any other confidential information. Additionally, to secure their cards, customers are advised not to reveal the security sign at the back of their cards when making transactions at the bank.

To prevent digital security risks arising from the use of the bank's mobile application, the bank incorporates state-of-the-art technology to make the application secure. As part of the technology, the bank ensures that the application has an SMS notification feature to alert customers whenever there is suspicious activity in their accounts (Rabita Bank, n.d.). Moreover, when accessing the application, customers are required to input their PIN codes, which are only known to them. This feature ensures that people who are not authorized cannot access the application from someone else's phone because they will be required to input the PIN code, which they may not have.

To prevent risks arising from Internet banking, the bank has incorporated a special security feature in the platform that ensures a double verification process. The double verification system ensures that one connects to the platform

by first entering a one-time password sent through SMS (Rabita Bank, n.d.). Next, the customer will be required to enter a one-time password that can be obtained from the ATM.

Besides customer education and awareness, the bank employs other measures to prevent credit and debit card fraud. These measures include the use of a 3-D secure system, E-PIN functions, and security certificates from certified associations like Visa and Mastercard (Rabita Bank, n.d.).

### Conclusion

The advancement in technology has seen almost every bank in Azerbaijan and the world embrace digital transformation to improve their operations and enhance customer experience. However, the digital transformation in banks has come with a number of risks. Some of these risks include operational disruptions, cyber security threats, and lack of regulatory compliance, among others. To mitigate or prevent these risks, banks must embrace some proven best practices. These best practices include leveraging other technologies like pilot programs, ensuring compliance with regulations and laws, conducting a comprehensive risk assessment, and investing in proper cyber security measures. Besides utilizing best practices in managing digital transformation in banks, banks must learn from other banks that have successfully managed their digital transformation. In Azerbaijan, one of these banks is the Rabita bank.

Rabita Bank embraced digital transformation in 2012. Since then, the bank has had its fair share of its benefits and challenges. Some of these challenges include cyber security threats, identity theft, and data breaches. To address these challenges, it incorporated customer education and awareness materials in its website to educate customers about the potential risks and how to avoid them, adopted advanced security technologies, ensured certification from authorized associations, and incorporated more advanced security measures like double verification. Through customer education, the customers are educated on how to identify suspicious links and the next steps to take in such a scenario. The double verification features ensure that people's data are protected from unauthorized access since it is more difficult to by-pass such a system compared to single verification. The certification by international card associations ensures that the cards are of the required state.

Digital transformation seems unavoidable in the banking sector because of the various benefits that it brings. While most banks are prepared to address known challenges, more research should be conducted to identify other unidentified threats, ensure seamless operations, and protect customers' data.

### References

1. Abbasov A, Mamedov Z. Digitalization of the banking sector: new challenges and prospects. *Econ Manag.* 2019;10(3):81-89.
2. Agarwal V, Butler C, Degenaro L, Kumar A, Sailer A, Steinder G. Compliance-as-code for cybersecurity automation in hybrid cloud. *J Open Innov Technol Mark Complex.* 2021;7(3):12-23.
3. Betz L. An analysis of the relationship between security information technology enhancements and computer security breaches and incidents [dissertation]. Florida: NSU Works; c2016.
4. California Management Review. To pilot or not to pilot - that is the question. New York: Insight; c2018.
5. Capgemini. Data privacy in the financial services industry. Paris: Capgemini; c2011.
6. Financial Services Information Sharing and Analysis Center. Ransomware, supply chain, Trojans drive cyber risk for Asia Pacific financial firms [Internet]. Financial Services Information Sharing and Analysis Center; 2019 [cited 2022 Jan 26]. Available from: <https://www.fsisac.com/newsroom/ransomware-supplychain-trojans-drive-cyber-risk-for-apac-financial-firms>
7. Kitsios F, Giatsidis I. Digital transformation and strategy in the banking sector: evaluating the acceptance rate of e-services. *J Open Innov Technol Mark Complex.* 2021;7(3):204-17.
8. KPMG International. Global banking fraud survey. Bern: KPMG; c2019.
9. Ponemon Institute. Data risk in the third-party ecosystem: third annual study. Traverse City: Ponemon Institute; c2018.
10. PWC. Caribbean digital readiness survey 2021. London: PWC; c2021.
11. Rabita Bank. Your safety is protected! [Internet]. Rabita Bank; n.d. [Cited 2022 Jan 2]. Available from: <https://www.rabitabank.com/individual-customer/security>