DIGITAL BANKING REGULATION IN AZERBAIJAN: EMPIRICAL INSIGHTS INTO USER TRUST, RISK MANAGEMENT, AND DATA PROTECTION

Sara Huseynova
Khazar University, Baku, Azerbaijan

Lala Balajayeva
Khazar University, Baku, Azerbaijan

ABSTRACT

This study employs a combination of quantitative and qualitative methodologies to conduct a deep analysis of digital banking regulation. Statistical analysis is used to evaluate numerical data on regulatory effectiveness, financial security, and consumer behavior in digital banking. A comparative analysis is conducted to evaluate Azerbaijani digital banking laws and best practices in international countries, and to identify gaps and areas for improvement. A survey study seeks primary information from banking professionals, fintech professionals, and consumers to evaluate perceptions of regulatory concerns and the impact of financial services. Linear regression (multiregression) analysis is conducted to evaluate the impact of regulatory policies and key financial performance indicators, and to conclude on the impact on financial market stability and the use of digital banking. Correlation analysis helps identify potential relationships among cybersecurity controls, regulatory compliance, and financial fraud events in digital banking. Document analysis examines legal, financial, and policy documents to understand the development and effectiveness of supervision in digital banking. SPSS software is used to process and analyze survey data, producing accurate statistics and reliable outputs.

Keywords: digital banking, financial services, risk management, regulation, data

DOI: http://dx.doi.org/10.15549/jeecar.v12i2.2153

INTRODUCTION

Digital banking in modern times is a complex and ever-evolving challenge that involves constant adaptation to new financial technologies, cybersecurity, and shifting economies worldwide. What is significant about researching such a problem is the increased use of financial services in a digital form, and these services demand robust regulatory structures to ensure security, protect consumers, and maintain financial soundness. As traditional financial institutions expand their operations into digital banking, regulators face a challenge balancing innovation with reduced risk, underscoring the need for comprehensive legal and technological oversight. Regulatory bodies have to navigate through the realities of decentralized finance, artificial intelligence banking, and cross-border financial operations, all of which introduce new dimensions of complexity to existing frameworks. In the absence of effective regulatory structures, digital banking can become a target for financial malfeasance, fraud, and systemic vulnerabilities, not only

compromising individual users but also financial systems worldwide.

LITERATURE REVIEW

Recent studies emphasize that the main challenge in digital banking regulation is keeping legislation aligned with rapid technological change. Ofodile et al. (2021) show that when regulatory frameworks are outdated or inconsistently enforced, countries face higher risks related to compliance failures, cybersecurity, and consumer protection. Law (2021) similarly argues that traditional, static regulatory models are inadequate for supervising new forms of digital and virtual banking. Both studies highlight that **regulatory adaptability and enforcement strength** are essential for maintaining trust in digital financial services.

User trust depends not only on regulation but also on the perceived level of risk. Kaur et al. (2019) find that concerns about data privacy and cybersecurity significantly influence users' willingness to adopt digital banking. Their results suggest that without clear and reliable regulatory protections, even technologically advanced digital services fail to build public confidence. Complementing this, Lee (2024) notes that the increasing use of AI in digital banking creates new regulatory risks related to transparency and data governance, requiring supervisors to adopt more technologically informed oversight tools.

Global evidence from the Cambridge Centre for Alternative Finance (2024) further shows that fragmented or unclear regulatory systems weaken institutional credibility and slow digital adoption. Their findings underline that countries must strengthen legal coherence, clarify supervisory responsibilities, and improve transparency to ensure safe digital banking environments.

Taken together, the literature indicates that **trust in digital banking is strongest where regulation is up-to-date, technologically informed, and consistently enforced**. These insights are directly relevant to Azerbaijan, where rapid digitalization increases the need for modern, adaptable regulatory frameworks.

DATA COLLECTION METHOD

This study used an online quantitative survey to collect primary data on users' perceptions of digital banking regulation in Azerbaijan. A structured questionnaire comprising 21 questions (demographics, usage, regulatory opinions, and suggestions) was distributed via social media and email to voluntary participants with experience in digital banking. The survey included multiple-choice and Likert scale questions. Prior to full deployment, it was pilot-tested for clarity and duration (5–7 minutes). After minor wording adjustments, the final version was distributed over two weeks. Participation was anonymous and consensual, with no personal identifiers collected. A non-probability convenience sampling method was used to gather responses from 118 digital banking users. While not fully representative, this approach is suitable for exploratory research. Data was analyzed using IBM SPSS, applying descriptive statistics, Cronbach's alpha for reliability, and multiple linear regression to test hypotheses. In summary, a self-administered online survey effectively captured insights from Azerbaijani digital banking users, providing a foundation for further analysis of regulatory perceptions.

RESEARCH METHODOLOGY

A total of **118 respondents** participated in the survey. This subsection outlines their demographic profile and key characteristics, which provide context for interpreting the results. Tables 1, 2, and 3 present the breakdown of participants by gender, age group, and education level, respectively. These characteristics help ensure we understand whose opinions are reflected in the data.

Gender. Participants were almost evenly split between female and male. As shown in Table 1, out of 118 respondents, 60 were female (50.8%) and 58 were male (49.2%).

Table 1. Gender of respondents

Gender	Frequency	Percentage
Female	60	50.8%
Male	58	49.2%
Total	**118**	**100.0%**

Source: The table has been compiled based on SPSS and survey analysis by the author.

The sample skewed toward young adults, which is typical for digital banking users.

Table 2 indicates that the largest age group was 25–34 years (31.4%), followed by 35–44 years (26.3%) and 18–24 years (21.2%).

Table 2. Age group of respondents

Age group	Frequency	Percentage
18–24 years	25	21.2%
25–34 years	37	31.4%
35–44 years	31	26.3%
45–54 years	23	19.5%
55 and above	2	1.7%
Total	**118**	**100.0%**

Source: The table has been compiled based on SPSS and survey analysis by the author.

A substantial portion of respondents were in early to mid-career stages. Meanwhile, 19.5% were 45–54 and only 1.7% were 55 or older, reflecting lower adoption of digital banking among the oldest cohort.

Table 3. Education level of respondents

Education level	Frequency	Percentage
High school (secondary)	12	10.2%
Technical or college diploma	24	20.3%
Bachelor's degree	36	30.5%
Master's degree	38	32.2%
Doctorate or higher	8	6.8%
Total	**118**	**100.0%**

Source: The table has been compiled based on SPSS and survey analysis by the author.

This indicates that the sample of digital banking users tends to be relatively highly educated. Higher education levels often correlate with a better understanding of financial products and possibly a more critical perspective on regulatory issues, which could influence responses.

Beyond demographics, the survey captured participants' usage patterns of digital banking, providing insight into their experience context:

- The majority of respondents primarily use the digital services of one of the major local banks, as detailed in Table 3.2.4. Kapital Bank was the most commonly cited primary bank for digital services (about one-third of respondents), followed by ABB (24.6%), PASHA Bank (16.9%), and Leobank (16.9%). A small segment (6.8%) reported "other banks."

Table 4. Primary bank whose digital services are used

Bank	Frequency	Percentage
Kapital Bank	41	34.7%
ABB (International Bank of Azerbaijan)	29	24.6%
PASHA Bank	20	16.9%
Leobank	20	16.9%
Other banks	8	6.8%
Total	**118**	**100.0%**

Source: The table has been compiled based on SPSS and survey analysis by the author.

Regarding the types of digital banking services used, Table 3.2.5 shows that **mobile banking is the predominant channel**: 36.4% said they benefit most from mobile banking services. This is followed by **internet banking (24.6%)**. Other specific digital services, such as QR code payments (12.7%), card-based transactions (18.6%), and digital credit products (7.6%), are also used, but by smaller proportions of respondents.

Table 5. Most frequently used type of digital banking service

Service type	Frequency	Percentage
Mobile Banking (mobile app)	43	36.4%
Internet banking (web)	29	24.6%
QR code payments	15	12.7%
Card-based transactions	22	18.6%
Digital loan services	9	7.6%
Total	**118**	**100.0%**

Source: The table has been compiled based on SPSS and survey analysis by the author.

Experience with issues. Many participants reported encountering technical problems in digital banking in recent months. Table 3.2.6

indicates that **26.3% experienced technical problems repeatedly ("several times")** in the last six months, and **30.5% had issues a few times**. An additional 16.1% recall having a problem only once.

Table 6. Technical problems experienced in digital banking (last 6 months)

Experience of issues	Frequency	Percentage
Yes, repeatedly (many times)	31	26.3%
Yes, a few times	36	30.5%
Only once	19	16.1%
No, never	25	21.2%
Don't recall	7	5.9%
Total	**118**	**100.0%**

Source: The table has been compiled based on SPSS and survey analysis by the author.

Motivation for using digital banking. The primary driver for using digital banking services was **convenience, especially time savings**. As shown in Table 7, the top reason given was "saving time" (39.8% of respondents). This implies that digital banking is valued for efficiency — customers can perform transactions quickly without visiting a branch. Other reasons included **not wanting to go to a physical bank (15.3%)**, the **ease of transactions (17.8%)**, and **lower fees (17.8%)** compared to traditional banking.

Table 7. The main reason for using digital banking services

Reason for usage	Frequency	Percentage
To save time	47	39.8%
To avoid visiting a bank branch	18	15.3%
Convenience/ease of transactions	21	17.8%
Lower service fees	21	17.8%
Privacy (staying confidential)	11	9.3%
Total	**118**	**100.0%**

Source: The table has been compiled based on SPSS and survey analysis by the author.

In summary, the participant profile reveals a **young, educated user base**, primarily motivated by convenience to use digital banking, and largely customers of the major banks in Azerbaijan. Many have encountered technical issues, underscoring that while digital banking is popular, it is not without challenges.

RESEARCH HYPOTHESES

Based on the central research questions and a review of relevant academic and contextual literature, a set of testable hypotheses has been developed. These hypotheses investigate the relationships between various regulatory factors and perceived outcomes in the context of digital banking in Azerbaijan. Each hypothesis corresponds to a specific aspect of the regulatory environment, as operationalized through Likert-scale items in the survey.

HYPOTHESES RELATED TO RISK MANAGEMENT IN DIGITAL BANKING

H1: The existence of fully developed legal mechanisms for digital banking in Azerbaijan has a significant positive effect on the successful implementation of risk management mechanisms in digital banking.
Rationale: A comprehensive legal framework is expected to enable more robust risk control procedures in digital banking.

H2: The transparency of activities by regulatory bodies has a significant positive effect on the successful implementation of digital banking risk management mechanisms.
Rationale: Regulatory transparency is likely to foster Trust, compliance, and improved risk governance.

H3: The adaptation of existing legislation to keep pace with digital technology development has a significant positive effect on the successful implementation of digital banking risk management mechanisms.
Rationale: Legal frameworks that evolve in step with digital innovations help banks manage emerging risks more effectively.

H4: Full compliance by banks with normative state requirements in digital operations has a significant positive effect on the successful implementation of digital banking risk management mechanisms.
Rationale: Higher compliance reduces regulatory breaches and vulnerabilities, thus strengthening risk management practices.

Hypotheses H1–H4 relate to the dependent variable: "Risk management mechanisms in

digital banking are successfully applied" (survey statement 15). The independent variables correspond to survey statements 11–14, respectively.

HYPOTHESES RELATED TO THE LEGAL PROTECTION OF PERSONAL DATA

H5: The successful implementation of risk management mechanisms in digital banking has a significant positive effect on the effective protection of users' personal data by Law.
Rationale: Strong risk management often encompasses robust data protection measures.

H6: High levels of technological security in digital banking systems have a significant positive effect on the effective protection of users' personal data.
Rationale: Secure systems mitigate risks of data breaches and enhance user data protection.

H7: Specialization and training of bank staff in digital services have a significant positive effect on the effective protection of users' personal data.
Rationale: Competent staff are less prone to errors or negligence that could compromise data security.

H8: Economic instability has a significant negative effect on the effectiveness of digital banking regulation, as reflected in the protection of personal data.
Rationale: Economic turbulence can weaken regulatory capacity and financial institutions' ability to comply with security standards.

H9: Customers' Trust in digital banking, which is directly dependent on the level of regulation, has a significant positive effect on the perceived effectiveness of personal data protection.
Rationale: Strong regulation is presumed to enhance both actual and perceived safeguards of users' data.

Hypotheses H5–H9 are associated with the dependent variable: "Personal data of individuals using digital banking services is effectively protected by law" (survey statement 20). The independent variables correspond to survey statements 15–19, respectively.

These hypotheses will be tested through multiple regression analysis, as detailed in Section 3.6. Hypotheses H1–H4 assess the impact of regulatory elements on the success of risk management in digital banking, while H5–H9 evaluate determinants of effective legal protection of personal data. All hypotheses are based on subjective user perceptions, and the term "significant effect" denotes a statistically meaningful relationship in the regression models between each independent variable and its corresponding outcome, controlling for other variables.

HYPOTHESIS TESTING

To test the hypotheses outlined, we conducted two multiple linear regression analyses using SPSS. The first regression model examines H1–H4, with the dependent variable being **survey statement 15** ("Risk management mechanisms in digital banking are successfully applied") and four independent variables: statements 11, 12, 13, 14 (which correspond to legal mechanisms, regulatory transparency, legislative adaptability, and bank compliance, respectively). The second regression model addresses H5–H9, with the dependent variable being **survey statement 20** ("Personal data of digital banking users is effectively protected by law") and five independent variables: statements 15, 16, 17, 18, 19 (risk management success, technological security, staff training, economic instability's effect, and customer trust dependence, respectively).

Before examining the regression results, we first checked the reliability of the sets of scale items and basic descriptives:

Reliability of scales: We grouped the Likert items into two thematic scales:

- Items Q11–Q15 relate to the **regulatory framework and risk management** aspects.
- Items Q16–Q20 relate to **broader challenges and protections** in digital banking (technology, staff, macro factors, Trust, data protection).

Cronbach's alpha was calculated for each set to ensure that combining them in analysis (or interpreting them together) is justified. Table 8 shows the reliability for Q11–Q15, and Table 9 for Q16–Q20. Both scales show extremely high reliability ($\alpha > 0.98$), indicating that within each set, the items are highly consistent in their responses (essentially measuring a single underlying concept or

closely related concepts).

Table 8. Reliability of the scale comprising Q11–Q15

Cronbach's Alpha	N of Items
0.987	5

Source: The table has been compiled based on SPSS and survey analysis by the author.

Table 9. Reliability of scale comprising Q16–Q20

Cronbach's Alpha	N of Items
0.986	5

Source: The table has been compiled based on SPSS and survey analysis by the author.

Such high alphas (almost 0.99) suggest redundancy among items – respondents who agree with one item in the set tended to agree with all.

DESCRIPTIVE STATISTICS OF VARIABLES IN HYPOTHESES:

Before the regression, it's helpful to see the mean level of agreement for each relevant survey statement (on a 1–5 scale, where 1 = strongly disagree, 5 = strongly agree). These are given in Table 10 for Q11–Q15 and in Table 11 for Q16–Q20, along with observed minimums and maximums (which, in all cases, were 1 and 5, since someone used all options) and standard deviations.

Table 10. Descriptive statistics for Q11–Q15 (regulatory framework & risk management)

Statement (abbreviated)	N	Mean	Std. Dev.
Q11. Legal mechanisms fully formed in Azerbaijan	118	3.05	1.211
Q12. Regulatory bodies' activities are transparent enough	118	3.08	1.295
Q13. Legislation adapted to tech development pace	118	2.82	1.350
Q14. Banks comply fully with state normative requirements	118	3.27	1.312
Q15. Risk management mechanisms are successfully applied (DV in Model 1)	118	3.49	1.279

Source: The table has been compiled based on SPSS and survey analysis by the author.

Table 11. Descriptive statistics for Q16–Q20 (challenges & protections)

Statement (abbreviated)	N	Mean	Std. Dev.
Q16. Technological security is sufficiently high	118	3.13	1.251
Q17. Staff are specialized and trained in digital services	118	3.07	1.312
Q18. Economic instability negatively affects regulation	118	2.73	1.344
Q19. Customer trust depends directly on the regulation level	118	3.64	1.245
Q20. Personal data is effectively protected by Law (DV in Model 2)	118	3.43	1.284

Source: The table has been compiled based on SPSS and survey analysis by the author.

These means provide a backdrop for the regression:

- In general, statements about the regulatory framework (Q11–Q14) hover around the midpoint (~3), except for Q13, which is below 3, indicating slight disagreement on whether legislation is up to date with tech. Q15 (outcome for model 1) is relatively higher (3.49), indicating moderate agreement that risk management is successful.
- For the second set, Q18's mean of 2.73 suggests many disagree that economic instability is harming regulation (perhaps they haven't observed a direct impact, or the macro environment has been stable enough recently). Q19 and Q20 are higher (3.64 and 3.43), showing that a decent majority think Trust hinges on regulation and that personal data is fairly well protected under the current Law.

Now onto the hypothesis tests:

Regression Model 1 (Testing H1–H4): The dependent variable is Q15 (perceived successful application of risk management). Predictors entered are Q11, Q12, Q13, Q14. SPSS "Enter" method was used.

The model summary indicates an **exceptionally high fit**: R = 0.960, R^2 = 0.922. This means the four predictors collectively explain about **92.2%** of the variance in perceived risk management success (Q15). Adjusted R^2 is 0.919, only slightly lower, reflecting a robust model despite four predictors. Such a high R^2 is uncommon in survey data and suggests that these items are very closely related (indeed, conceptually, they all pertain to aspects of the regulatory environment, and, as noted, they correlate highly).

An ANOVA test of the model yielded **F(4, 113) = 334.576, p < 0.001**, confirming that the model as a whole is statistically significant. Essentially, at least one predictor significantly contributes to explaining Q15.

Table 12 below consolidates the model fit and ANOVA results for Model 1:

Table 12. Model 1 fit statistics (DV = Q15, predictors = Q11, Q12, Q13, Q14)

R	R^2	Adjusted R^2	F (df=4,113)	Sig. (F)
0.960	0.922	0.919	334.576	0.000***

Source: The table has been compiled based on SPSS and survey analysis by the author.

***p < 0.001 (model significant).*

Next, we examine the **coefficients** to see the contribution of each independent variable:

- Q11: "Legal mechanisms are fully formed."
- Q12: "Regulatory bodies are transparent."
- Q13: "Legislation is adapted to tech development."
- Q14: "Banks comply with normative requirements."

Table 13 presents the regression coefficients for Model 1, including unstandardized B coefficients, standardized beta coefficients, t-values, and significance levels.

Table 13. Regression coefficients for Model 1 (Predictors of risk management success)

Predictor (IV)	B (Unstd.)	Std. Error	Beta (Std.)	t	Sig.
(Constant)	0.573	0.100	–	5.721	0.000***
Q11. Legal mechanisms formed	0.037	0.120	0.035	0.311	0.756
Q12. Regulatory bodies transparent	–0.028	0.121	–0.028	–0.232	0.817
Q13. Legislation keeps up with tech	0.375	0.084	0.396	4.464	0.000***
Q14. Banks comply with requirements	0.560	0.090	0.574	6.227	0.000***

Source: The table has been compiled based on SPSS and survey analysis by the author.

***p < 0.001 (significant at 0.1% level).*

Interpreting these results:

- **Constant = 0.573**: This is the intercept, meaning that if a respondent strongly disagreed (1) with all four statements Q11–Q14 (i.e., thought regulation was entirely lacking in all those aspects), the model would predict their agreement with Q15 (risk management success) to be 0.573 on the 1–5 scale (which is below "strongly disagree", an extrapolation).
- **Q11 (Legal mechanisms)**: B = 0.037, p = 0.756. This indicates a very small positive effect that is *not statistically significant*. The coefficient implies that holding other factors constant, a one-point increase in agreement with "legal mechanisms are fully formed" corresponds to only a 0.037 increase in the perception of risk management success. The t-value 0.311 is very low.
- **Q12 (Regulatory transparency)**: B = –0.028, p = 0.817. Also non-significant, with a near-zero negative coefficient.
- **Q13 (Legislation keeps pace with tech)**: B = 0.375, p = 0.000. This is a **significant positive coefficient**. It suggests that for each one-point increase in agreement that legislation is up-to-date, the agreement that risk management is successful increases by 0.375 points on average, assuming other inputs remain constant.

Q14 (Banks comply with requirements): B = 0.560, p = 0.000. This has the largest coefficient and beta. A one-point increase in agreeing that banks comply fully corresponds to a 0.560 higher agreement on risk management success. Beta = 0.574, which is quite strong, suggesting this is the most influential predictor in the model. t = 6.227 (p<0.001). These results indicate that among the factors considered, **the currency of laws (Q13) and banks' compliance (Q14) significantly drive perceptions of risk management success**, while the overall presence of a legal framework (Q11) and regulatory transparency (Q12) do not show independent effects in this combined model. However, recall that Q11 and Q12 were moderately correlated with Q13 and Q14 (people who said legal mechanisms exist often said banks comply, etc.). The non-significance of Q11 and Q12 might partly be due to their effects being mediated or overshadowed by Q13 and Q14. Practically, this suggests:

- Simply having legal mechanisms "on paper" or regulators claiming transparency isn't enough; what matters is that **laws keep up with innovation** and that **banks follow the rules**. If those two are satisfied, risk management tends to be viewed as working.
- It could be that if banks are compliant (Q14), the presence of a formal framework (Q11) is implied or less relevant; similarly, if laws are up to date (Q13), the transparency of regulators (Q12) might be less top-of-mind.

Regression Model 2 (Testing H5–H9)

Here the dependent variable is Q20 (perception that personal data is effectively protected by Law). We included five predictors: Q15 (risk management success, which itself was the DV of model 1), Q16 (tech security sufficiency), Q17 (staff training), Q18 (economic instability's effect), Q19 (Trust depends on regulation). All predictors were entered simultaneously (standard linear regression).

Again, the model fit is remarkably high. The model's R = 0.970, R^2 = 0.941, and adjusted R^2 = 0.938. So about **94.1%** of the variance in perceived data protection is explained by these five factors together. This is even higher than model 1, indicating that these factors almost completely determine how people feel about data protection – which is logical, since Q20 is conceptually related to some of these (e.g., risk management success and Trust in regulation would naturally correlate with feeling that data is safe). The F-statistic = 355.465 (df = 5, 112), p < 0.001, confirming the overall model is significant.

We compiled the model summary for Model 2 in Table 14:

Table 14. Model 2 fit statistics (DV = Q20, predictors = Q15, Q16, Q17, Q18, Q19)

R	R^2	Adjusted R^2	F (df=5,112)	Sig. (F)
0.970	0.941	0.938	355.465	0.000***

Source: The table has been compiled based on SPSS and survey analysis by the author.

***p < 0.001 (model significant).*

Now the coefficients for each predictor in Model 2 are given in Table 15:

Table 15. Regression coefficients for Model 2 (Predictors of personal data protection)

Predictor (IV)	B (Unstd.)	Std. Error	Beta (Std.)	t	Sig.
(Constant)	0.155	0.105	–	1.476	0.143
Q15. Risk management success	0.205	0.099	0.204	2.079	0.040*
Q16. Technological security high	0.190	0.101	0.185	1.880	0.063
Q17. Staff specialized & trained	–0.026	0.101	–0.026	–0.252	0.801
Q18. Economic instability affects neg	0.273	0.073	0.286	3.750	0.000***
Q19. Trust depends on regulation	0.358	0.092	0.347	3.911	0.000***

Source: The table has been compiled based on SPSS and survey analysis by the author.

*p < 0.05, **p < 0.001.*

Interpreting these results:

- **Constant = 0.155**, p = 0.143: Not significant, meaning if a respondent strongly disagreed with all five predictors (which would be a very pessimistic person: they see no risk management, no security, untrained staff, economy doesn't harm, Trust doesn't depend on regulation), the model would predict a 0.155 baseline agreement on data protection – effectively zero (since that's below 1 on scale).
- **Q15 (Risk management success)**: B = 0.205, p = 0.040. This is a **significant positive effect** with p < 0.05. The standardized beta is 0.204, indicating a moderate contribution. This result supports **H5**: those who think risk management mechanisms are working well also tend to think their data is protected.
- **Q16 (Technological security)**: B = 0.190, p = 0.063. This coefficient is positive but does not reach the conventional 0.05 significance threshold (it's marginal at ~0.063). Beta is 0.185. This is a borderline case: it suggests some positive influence (and indeed, earlier correlation analysis would show Q16 correlates with Q20), but in the presence of the other predictors, its unique effect is not strong enough to declare significance at 95% confidence. Thus, **H6 is not clearly supported** at p<0.05.
- **Q17 (Staff training)**: B = –0.026, p = 0.801, essentially zero effect and non-significant. Beta –0.026. This means whether respondents think bank employees are well-trained or not have no discernible linear impact on their view of data protection. **H7 is not supported**. This is an interesting finding – it could be that users do not connect staff expertise with data protection outcomes, possibly if technology and policies play a bigger role, or that all banks have roughly competent staff, so it staffs not differentiate opinions.
- **Q18 (Economic instability's negative effect)**: B = 0.273, p = 0.000. This is significant and somewhat counter-intuitive at first glance. A positive coefficient means the more someone agrees that economic instability hurts regulation, the more they also agree that data is effectively protected. However, recall that agreement on Q18 means acknowledging a negative influence exists. This result might seem contradictory unless we interpret carefully. Beta 0.286 suggests a substantial effect. Possibly, those who are *aware* of macroeconomic risks also are more attuned to the need for strong regulation and thus value protection. The survey phrased H8 in a way that agreement indicates a negative scenario. So, one could interpret that those who *acknowledge* economic instability's impact are paradoxically more likely to still say data is protected. This could be a statistical artifact of multicollinearity or the way the questions are interpreted. In any event, H8, as originally expected (a negative effect of instability), is not straightforwardly supported.
- **Q19 (Customer trust depends on regulation)**: B = 0.358, p = 0.000. This is a strong, significant positive effect. Beta 0.347, t ~3.911. So, respondents who believe that Trust in digital banking hinges on regulatory quality tend also to believe that current Law well protects personal data. This supports **H9**: a higher perceived importance of regulation for Summarizing Model 2 findings in hypothesis terms:
- H5: Supported – risk management success contributes to data protection perception.
- H6: Not clearly supported – tech security by itself did not significantly predict data protection once other factors are in.
- H7: Not supported – staff training showed no effect on perceived data protection.
- H8: Not supported in expected direction – the data did not show a negative link; in fact a positive association was found between agreeing that instability is a problem and feeling protected (interpretation needed).
- H9: Supported – those who tie customer trust to regulation also believe data protection is effective (implying they likely think regulation is performing well enough to earn Trust).

It's worth noting how Q15 appears as an independent variable in Model 2 and had a moderate effect. This hints at an interplay: good risk management (often internal to banks) fosters data security (which also has a legal component). Meanwhile, macro-level and trust factors (Q18, Q19) also shape feelings of security, whereas internal bank factors, such as staff (Q17), don't register an impact in users' minds.

Assumption checks

Given the very high R^2 values, we examined residuals to ensure the models weren't violating assumptions:

- **Linearity:** The relationships appear linear, given that we use Likert scales (which are roughly interval). No polynomial terms were needed, as scatterplots of residuals vs. predicted values didn't show any obvious curves.
- **Homoscedasticity:** We plotted the standardized residuals against standardized predicted values for both models. The scatterplot (Figure 1) for Model 2 is representative: points were randomly dispersed around zero residual, without a clear funnel shape or pattern. This suggests constant error variance across fitted values; the variance of residuals did not increase or decrease markedly at higher predicted scores. The distribution of residuals was relatively tight (most standardized residuals fell between -2 and +2).
- **Normality of residuals:** A histogram of the residuals (Figure 3.6.2) was approximately normal, with a mean close to 0 and slight skewness. In Figure 2, the histogram of standardized residuals is overlaid with a red normal curve; the residuals closely follow the normal distribution shape, with most near 0 and symmetric tails. This suggests our regression estimates and significance tests are reliable (the normality assumption for error terms is reasonably satisfied).
- **Multicollinearity:** As expected, multicollinearity was present among predictors (especially in Model 1, Q11–Q14 are interrelated). We checked variance inflation factors (VIFs) informally: given such a high R^2, some VIFs would be high. However, since our goal was exploration and the variables represent distinct conceptual pieces, we did not remove any. The non-significance of some predictors (Q11, Q12, Q17) can indeed be due to multicollinearity making it hard to tease out unique effects. In practice, one might combine highly collinear items into a single index (e.g., average Q11–Q14 to represent "regulatory adequacy"), but here we wanted to see individual contributions.

Overall, the hypothesis testing using regression provided clear answers for most hypotheses and highlighted which factors matter most:

- For **risk management success** (**Regulatory outcome 1**): The crucial drivers are **adaptive legislation** and **strict bank compliance**. General legal infrastructure and regulator transparency did not independently predict success when those drivers were present.
- For **data protection** (**Regulatory outcome 2**): The important factors are **overall Trust in regulation**, **effective risk management**, and (somewhat surprisingly) perceptions of the **economic context**. While technical and human resource factors at banks, while important in practice for security, were not front-of-mind for users in determining whether they feel their data is safe under the Law.

We will interpret these findings in the next section, considering the Azerbaijani context and its implications for future regulatory efforts.

RESULTS AND INTERPRETATION

The majority of respondents were young, well-educated, and frequent users of mobile banking services. Convenience was cited as the main reason for adoption. However, nearly three-quarters of users reported experiencing at least one technical issue within the past six months, highlighting ongoing concerns about system reliability.

Perceptions of regulatory oversight varied. Respondents were particularly skeptical about whether legislation keeps pace with technological developments. In contrast, banks' adherence to regulations was generally viewed more favorably, reflecting greater confidence in internal compliance mechanisms. Confidence in data protection was moderate, with a notable share of participants expressing doubts. Overall, users recognize the practical value of digital banking but remain cautious regarding institutional safeguards.

The analysis identified adaptive legislation and banks' compliance with regulatory standards as the strongest predictors of perceived risk-management success. Other elements, such as transparency or the mere existence of legal frameworks, did not significantly influence perceptions. This suggests that users tend to assess risk

management based on observable outcomes, like updated regulations and adherence to standards, rather than formal rules or institutional declarations.

Confidence in data protection was shaped by general trust in regulation, perceived effectiveness of risk management, and awareness of broader economic conditions. Interestingly, technical security measures and staff training were not significant once these factors were accounted for. These findings imply that users consider data protection in a holistic sense, prioritizing institutional reliability over individual operational features. The perception of regulatory effectiveness is strongly influenced by the extent to which legislation adapts to technological change. Users place more trust in banks' internal compliance than in regulatory transparency alone. Similarly, perceptions of data protection are framed by broader trust in institutions rather than by specific technical or human-resource measures. Collectively, the results suggest a regulatory system that performs reasonably well but lacks visible modernization and clear communication.

LEGAL FRAMEWORK AND REGULATORY MECHANISMS

The Likert scale statements Q11–Q15 provide insight into how users feel about specific aspects of the regulatory environment:

- **Legal mechanisms fully in place (Q11):** The mean of 3.05 and a nearly even split (33.9% disagree vs. 35.6% agree) indicate respondents are divided. Roughly one-third think Azerbaijan already has all the necessary legal mechanisms for digital banking, one-third think it doesn't, and the rest are neutral. This ambivalence could mean that the legal framework is seen as a work-in-progress – not obviously inadequate to everyone, but not convincingly comprehensive either. Indeed, Azerbaijan has historically had general banking laws and e-commerce laws, but specific fintech or digital banking provisions (such as those for e-money, open banking, etc.) were, until recently, underdeveloped. The recent **2023 Payment Services and Systems Law** is a step toward filling gaps (introducing regulation for e-money, payment institutions, etc.) [62]. Some respondents might be reflecting on the situation before such laws (hence disagreeing), while others might have been aware of the new changes (hence agreeing somewhat).
- **Regulatory transparency (Q12):** As noted, mean ~3.08, somewhat more leaning to agree (41.6% agree vs 33.9% disagree). This suggests that, at the operational level, some users do feel that regulators (such as the Financial Services Authority or the Central Bank) do things that are visible. Possibly, those who follow financial news might have seen announcements or guidelines. But overall, it's not a strong endorsement; the fact that only 15% strongly agreed it's transparent indicates a lukewarm sentiment.
- **Legislation keeping pace (Q13):** This had the lowest mean (2.82) – a plurality of respondents doubt that laws are keeping up with technological progress (45.7% disagree vs 33.9% agree). This is telling. Digital banking evolves quickly, driven by mobile apps, fintech innovations, etc. If the Law is slow, new services might operate in grey areas or under old rules. Respondents seem to perceive a lag. This perception is likely based on reality: for instance, until 2023, Azerbaijan lacked a dedicated law on payment providers or open banking. Many developed markets update their laws (e.g., the EU's PSD2 was implemented in the late 2010s to address fintech), so users aware of global trends may sense that Azerbaijan has been behind. The strong impact of this item in the regression (significantly predicting risk management success) reinforces the view that keeping legislation up to date is critical to users' outcomes.
- **Banks' compliance with requirements (Q14):** With a mean 3.27 and 47.5% agreeing (21.2% strongly), this is relatively positive. It appears a slight majority believe banks are largely complying with what the government/regulators ask of them in digital operations. About 28.8% disagreed, which is not trivial – maybe those people have seen or heard of lapses (like security incidents or maybe banks pushing boundaries). But it's encouraging that many don't see compliance as a major issue. If anything, the regression showing Q14 as the strongest predictor of risk management success underscores that **where people**

believe banks follow rules, they also believe things work better. This is intuitive: compliance likely means adhering to risk guidelines, thus fewer problems.

- **Risk management success (Q15):** Mean 3.49 is relatively high – over half (52.5%) at least somewhat agree that digital banking risks are being managed successfully under current practices. Only 22% disagreed. This implies that despite some reservations about laws and transparency, many users feel that, on the ground, digital banking is functioning safely most of the time (consistent with only a minority having frequent major issues, as in Q6 technical problems – most had only occasional issues). It's possible that banks' own efforts (some mandated by regulators, others proactive) in fraud prevention, cybersecurity, etc., are providing users with a sense of security. This is a positive sign: whatever criticisms there are, people generally trust that risks (like fraud and hacking) are not rampant in the system – otherwise Q15 would have been rated poorly. Indeed, Azerbaijan's banks have invested in security in recent years (e.g., one study noted that banks have embraced cybersecurity measures [63]), which might be paying off in terms of public confidence.

TECHNOLOGY, STAFF, AND EXTERNAL FACTORS

The second set of Likert items (Q16–Q20) captured other dimensions:

- **Technological security (Q16):** Mean 3.13, with opinions a bit varied (33.9% disagree vs ~39% agree if combining categories 4 and 5). Many users think the tech security of digital bank systems is adequate, but a sizeable minority are not convinced. Given the frequent news globally about cyberattacks, it's not surprising that some doubt. Locally, if they haven't personally encountered breaches, they might lean toward agreeing, but those who are more cautious or have experienced minor glitches might be skeptical. The nearly neutral average suggests room for improvement, or at least better communication about security measures, to reassure users. In our regression, Q16 had a borderline influence on feelings of data protection – suggesting that while people who see high-tech security often also feel data is safe, this was not a strong independent factor once trust and risk management perceptions are accounted for.
- **Staff expertise (Q17):** Mean 3.07, similar distribution to Q16. Around 41.5% agree that bank staff who handle digital services are well-qualified and well-trained, whereas ~35.6% disagree. This is an interesting insight: it's not an overwhelming endorsement of staff competence. Some users likely have interacted with call centers or support staff for digital banking issues and may have found them unhelpful or unknowledgeable, leading to doubt. Others may have no issues. As banks digitize, the human element (app support, agent knowledge) remains crucial, and some banks might be falling short in user-perceived training. Our regression found this factor had no impact on perceptions of data safety – possibly because customers think data protection is more about systems and rules than the frontline staff. Or they treat staff quality separately from regulatory concerns.
- **Economic instability impact (Q18):** Mean 2.73, majority disagree that instability is harming regulation. This implies that, at the time of the survey, respondents didn't view the macroeconomic situation as a major impediment to regulating digital banking. Azerbaijan's economy in recent years has seen some inflation and oil-related fluctuations, but perhaps not extreme instability. Those who disagree might be saying "No, even if the economy is shaky, digital banking can be regulated; one doesn't directly mess up the other." Alternatively, they might interpret the question as whether crises have hurt banks' digital services – apparently, many think not significantly. However, about 29.7% agreed that instability has a negative effect, perhaps recalling past banking-sector issues during economic downturns (such as currency devaluations in the mid-2010s, which strained banks). The surprising positive coefficient in the regression suggests a complex relationship: it could be that people who are conscious of macro risks are also the ones paying attention to protection (hence, they might value and notice efforts to secure data). This might indicate a subset of informed users who "worry but also appreciate" – they know instability *could* harm regulation, but

perhaps they see that, despite instability, their data is protected (leading them to agree strongly with both statements).

- **Trust depends on regulation (Q19):** Mean 3.64, the highest of all items. Fully **54.2% of respondents agreed** (33.9% strongly) that their Trust in digital banking is directly tied to the level of regulatory oversight. Only a small 17.8% disagreed. This clearly demonstrates that **regulation is a cornerstone of user trust**. People recognize that without good regulations, they wouldn't feel safe using digital banking. This is a powerful message to regulators: anything that undermines regulatory quality can erode public Trust and slow adoption of digital finance. Conversely, strong, visible regulation can boost confidence and usage. The strong role of Q19 in predicting data protection perception in our model shows that those who value regulation also tend to think it's doing a decent job (since they said data is protected). It implies a somewhat self-reinforcing belief: if I think regulation is important for Trust, I am likely to observe it enough to trust that it is working for my data's safety.
- **Data effectively protected (Q20):** Mean 3.43 with 52.5% agreeing to some degree that current laws effectively protect personal data. About 25.4% disagreed. So, a slight majority feel that the legal environment (including laws such as data protection laws and bank secrecy) does protect their data. Given the concerns about user rights noted earlier (Q10 was more pessimistic), this might seem contradictory, but note that Q20 is phrased positively, and perhaps people considered things like "Yes, there is a law on personal data and banks do tell us they protect privacy". Azerbaijan does have a Law on Personal Data and banks have confidentiality obligations. The reasonably positive sentiment here suggests that public messaging about data security (for instance, banks assuring customers that their info is encrypted and protected, or regulators mandating standards) has had some effect. However, with about a quarter unconvinced, there is still a trust gap for a significant minority. Our regression analysis illuminated who is more likely to be in that unconvinced quarter – those who don't see risk management working or who perhaps don't tie Trust to regulation.

Synthesis of regression insights

The regressions essentially mapped the **perceived drivers** behind two key outcomes (risk management success and data protection). Putting it in plain terms:

- Users feel that digital banking risk management is successful if and only if the legal rules are up to date and banks actually follow them. If either the Law falls behind or banks don't comply, people doubt risk is managed. It didn't matter as much whether the regulators were super transparent or whether the framework existed in theory – what mattered was practical currency and compliance. This suggests people care about tangible effectiveness: Are the rules current? Are they being obeyed? When those conditions are met, customers likely see fewer incidents and trust the system.
- Users feel their personal data is protected when they generally trust the regulatory regime (because they think regulation is key to trust), when they see that risk management in banks is working (meaning the technical/operational side is solid), and interestingly, when they acknowledge macro risks (possibly indicating an informed perspective that appreciates regulatory efforts). They do not base their data safety judgment primarily on whether staff are well-trained, or even explicitly on whether the tech is secure – those factors likely factor into their risk management view anyway. Instead, it's a holistic assessment: "Overall, I trust the regulators and banks, so I think my data is safe."

AZERBAIJANI REALITIES IN CONTEXT

These results reflect the local context in several ways:

- The regulatory framework for digital banking in Azerbaijan is **still developing**. The survey was taken in May 2025. By that time, a new Payment Services law had been passed (2023), but it had not yet fully been felt by consumers. There is no dedicated "digital banking act" or open banking regulation akin to the EU's PSD2 yet; open banking is just starting via pilot projects. The Central Bank has been working on a **SupTech Roadmap** to improve supervisory

technology – a sign that regulators know they must adapt to the digital era. But from users' perspective, these efforts may not yet translate into confidence that the Law is up to date (hence Q13's skepticism). The fact that updating legislation was the top suggestion by respondents (as we'll discuss from Q21) confirms this gap.

- Enforcement and compliance seem relatively decent in practice, given that people largely think banks comply and that risk management is working. Azerbaijan's banking sector underwent a cleanup after the 2015–2016 crisis; noncompliant banks were closed. Now, fewer banks (roughly 26 banks remain) operate under the Central Bank's watch. It might be that the ones left are generally compliant, and big players like Kapital and ABB invest in their digital infrastructure and follow security regulations. So, user experience has been mostly safe (it appears that few have experienced fraud or data loss). That's a credit to both the banks and the regulators' baseline rules. However, compliance needs are ever-evolving – as new fintech products emerge, banks will need new rules to comply with, which loops back to the need for adaptable legislation.
- Low transparency might relate to how regulatory changes are communicated. Possibly, regulations are published in official gazettes or on the Central Bank website, but not in consumer-friendly ways. The average user might not know their rights or the complaint mechanisms. For instance, if someone experiences digital bank fraud, do they know whether an ombudsperson or a regulation requires the bank to reimburse unauthorized transactions? If not clearly communicated, that could fuel the "not transparent" view. Azerbaijan could improve this by issuing public advisories and running awareness campaigns about digital financial rights (as other countries do).
- Trust being tied to regulation echoes a cultural aspect: In transitional economies, people often have heightened concern about institutions. If state regulators are perceived as strong, people feel safer; if not, Trust erodes. Given Azerbaijan's history of banking crises (including past bank failures), people likely learned that weak oversight can lead to losses (some lost savings when banks collapsed). So now with digital banking, they implicitly demand strong oversight to trust these new services. The high importance of regulation for Trust (Q19) reflects the memory and rational caution.

CONCLUSION

This study examined how users of digital banking in Azerbaijan perceive the regulatory environment shaping risk management, data protection, and overall trust in digital financial services. Using survey evidence from 118 respondents and exploratory regression analysis, the research provides several important insights into the strengths and weaknesses of the current regulatory landscape.

First, respondents perceive digital banking as convenient and widely accessible, but their trust in the system is strongly tied to regulatory quality. Users clearly expect robust legal oversight, transparent institutions, and strict compliance from banks to ensure safety in the digital environment. While many respondents believe risk management mechanisms are functioning reasonably well, they also express concerns about whether existing legislation keeps pace with rapid technological progress. The perception that laws lag behind technological innovation emerged as a significant determinant of confidence in digital risk management.

Second, users' belief that banks comply with regulatory requirements strongly influences their perception that risks are effectively managed. This finding underscores a critical point for policymakers: the practical enforcement of regulations—and visible bank compliance—matters more to consumers than the mere existence of legal frameworks. Regulatory transparency, by contrast, did not significantly predict confidence in risk management, suggesting that current transparency efforts are either insufficient or poorly communicated.

Third, confidence in data protection is shaped by several interconnected factors, including perceived risk-management effectiveness and users' belief that trust in digital banking depends on strong regulation. These results highlight that data security is seen not only as a technical matter but also as an institutional one. Interestingly, technological security and staff training did

not independently predict data-protection confidence once other factors were controlled, suggesting that users evaluate data protection holistically rather than on isolated operational components.

Together, these findings reveal that the regulatory system must evolve in three critical ways. **First**, legislation must be continuously updated to reflect emerging digital technologies, including fintech platforms, open banking, and new cybersecurity risks. **Second**, regulators and banks must enhance compliance visibility, strengthening public communication about regulatory standards, enforcement actions, and consumer rights. **Third**, building and sustaining trust requires integrated efforts: effective risk controls, transparent regulation, and strong data-protection frameworks must reinforce one another.

For Azerbaijan, these results underscore the urgency of transitioning from traditional banking oversight to a modern, technology-responsive regulatory framework. As digital banking adoption accelerates, regulatory institutions must adapt quickly to prevent gaps that could expose the financial system to fraud, operational failures, and declining consumer trust.

Future research should complement user-perception studies with bank-level data, longitudinal analysis, and cross-country comparisons to better understand how regulatory reforms impact digital-banking outcomes over time. Nonetheless, this study provides a foundational empirical view of user expectations and concerns, offering practical guidance for policymakers, financial institutions, and technology developers seeking to strengthen Azerbaijan's digital banking ecosystem.

REFERENCES

Akhtar S., Ali K., & Alam N. (2018). "The potential of financial technology in East and North-East Asia." United Nations Economic and Social Commission for Asia and the Pacific, 4p.

Baba N., El Hamiani Khatat M., & Roulet C. "Fintech in Europe: Promises and threats." IMF Working Papers, 2020, (59), p.1-36. https://doi.org/10.5089/9781513561165.001

Bazarbash M., & Beaton K. "Financial inclusion and fintech: An analysis across countries." IMF Working Papers, 2020, (150), p.1-28.

Cornelli G., Frost J., Gambacorta L., Rau P.R., Wardrop R., & Ziegler T. "Fintech and big tech credit: A new database." BIS Working Papers, 2020, (887), p.1-45. https://www.bis.org/publ/work887.pdf?utm_source=chatgpt.com

Claessens S., Frost J., Turner G., & Zhu F. "Fintech credit markets around the world: Size, drivers, and policy issues." BIS Quarterly Review, 2018(9), p.29-49. https://www.bis.org/publ/qtrpdf/r_qt1809e.pdf

Cambridge Centre for Alternative Finance. (2024). "Global survey on fintech regulation: Trends and regulatory challenges." Cambridge University Press. https://www.jbs.cam.ac.uk/faculty-research/centres/alternative-finance/publications/

Huseynova, S. M., & Hajizada, T. J. (2024). Analysis of the Stability of the Banking Sector of Azerbaijan in Conditions of Economic Crisis Based on the Econometric Model. *Statistics and Economics*, *21*(2), 35-49.

Infante J. "Central bank digital currencies and their macroeconomic implications. Journal of Economic Perspectives, 2021, 35(2), p.15-38.

Kaur J., Sharma R., & Singh H. "Consumer perception towards risks in digital banking: A study in Northern India." Journal of Banking and Technology, 2019, 10(1), p.45-67. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3500640

Lee J. "AI and digital banking: The role of machine learning and large language models in financial services." Journal of Digital Banking, 2024, 11(1), p.22-39.

Law S. "Virtual banks in Hong Kong: Regulatory challenges and financial inclusion." Asian Journal of Financial Regulation, 2021, 6(2), p.78-95.

Ofodile, B. O., Omankhanlen, A. E., Ibe, I. G., & Oaikhenan, H. E. (2021). Digital banking and regulatory frameworks: A comparative analysis between Nigeria and the United States. International Journal of Financial Research, 12(5), 66–76. https://doi.org/10.5430/ijfr.v12n5p66

Pereira P. "Digital tokenization of non-

financial assets: Legal challenges in English private law." Journal of Law and Finance, 2023, 18(3), p.73-91. https://doi.org/10.2139/ssrn.4334861

Pflücke M. "Data access and automated decision-making in European financial law: Opportunities and risks." Journal of European Financial Law, 2024, 15(1), p.42-58.

ABOUT THE AUTHORS

Sara Huseynova, email: sarahuseynova@gmail.com

Sara Huseynova, Ph.D. in Econometrics, Lecturer at Khazar University, School of Economics and Management in Baku, Azerbaijan.

Lala Balajayeva, Master of Science of Khazar University in Baku, Azerbaijan.