



Cybersecurity Governance in Islamic Digital Banking: A Maqashid al-Sharia Perspective

Imelda Aisyah^{1*}, Lely Ana Ferawati Ekaningsih²

^{1,2} Universitas KH. Mukhtar Syafaat Banyuwangi, Indonesia

Article Info	Abstract
Article history: Received March 10, 2026 Revised April 13, 2026 Accepted June 27, 2026 Available online August 15, 2026 *Corresponding author email: imeldaaisyah05@gmail.com Keywords: Bank Muamalat, Cybersecurity, Digital Services, Maqashid al- Sharia, Maslahah	Introduction/Main Objectives: This study analyzes the implementation of cybersecurity in Bank Muamalat's digital services from a maqashid al-sharia perspective, examining its alignment with the protection of customers' wealth, soul, and intellect in the realization of maslahah. Research Methods: This qualitative case study at Bank Muamalat Genteng Banyuwangi employed in-depth interviews, observation, and documentation with eight purposive informants. Data were analyzed using Miles and Huberman's interactive model with source and method triangulation. Finding/Results: Bank Muamalat implements cybersecurity measures in its Digital Islamic Network, reflecting <i>hifz al-mal</i> (wealth protection), <i>hifz al-nafs</i> (soul protection), with active user growth, and <i>hifz al-'aql</i> (intellect protection) through customer education, aligning with QS. Al-Maidah (5:90), which prohibits acts that destroy the intellect and the soul. Customers express satisfaction, although generational literacy gaps persist. Conclusion: Cybersecurity is crucial for realizing maslahah in Islamic digital banking. Integrating maqashid values and inclusive customer education is key to maintaining trust.
Page: 61-71	AICIE with CC BY license. Copyright © 2026, the author(s)

INTRODUCTION

Digital transformation has fundamentally altered the landscape of the banking industry. Islamic banking, grounded in Islamic principles, cannot overlook this wave of digitalization. (Rofiullah, 2025; Sarpini, 2025). Bank Muamalat Indonesia (BMI), the first Islamic bank in Indonesia, established in 1991, has taken a strategic step by introducing the Muamalat DIN (Digital Islamic Network) application as its premier digital service. (Bank Muamalat Indonesia, 2024). By November 2025, Muamalat DIN had been downloaded over one million times and featured more than 250 functions designed to support various customer transaction needs. (Bank Muamalat Indonesia, 2025). Moreover, over 90% of Bank Muamalat customer transactions are now conducted through digital channels, indicating a significant shift in customer behavior from conventional to digital services. (Maulia et al., 2025).

Banking digitalization increases cybersecurity risks, threatening customer trust and security. (Utami, 2026; Putri et al., 2025). Cybercrimes in the banking sector continue to evolve with increasingly sophisticated methods, ranging from phishing and social engineering to system hacking that can result in significant financial losses. (Hutagalung et al., 2025). Data from the Financial Services Authority (OJK) indicates that cybercrime cases in the financial services sector have grown exponentially over the past three years, with losses reaching trillions of rupiah. (OJK, 2023). This phenomenon not only threatens the stability of the national financial system but also has the potential to undermine public trust in digital banking services, including Islamic banking. (Supriadi et al., 2025; Zulika et al., 2025).

In the context of Islamic banking, cybersecurity is not merely a technical issue but possesses profound ethical and spiritual dimensions related to the protection of customers' wealth, soul, and intellect. (Rofiullah, 2025). Unlike conventional banking, which is oriented solely toward profit, Islamic banking bears a dual responsibility: compliance with technical regulations while fulfilling sharia principles that prioritize justice, transparency, and protection of public interest ((Kurnia et al., 2025; Maulia et al., 2025). Cybersecurity failure in Islamic banking not only causes material losses but can also damage the image of Islamic banking as a trustworthy and reliable financial institution. (Hutagalung et al., 2025).

The principles of maqashid al-sharia, which aim to protect religion (*hifz al-din*), soul (*hifz al-nafs*), intellect (*hifz al-'aql*), lineage (*hifz al-nasl*), and wealth (*hifz al-mal*), provide an essential framework for assessing the implementation of cybersecurity in Islamic banking. (Rofiullah, 2025; Kurnia et al., 2025). Effective cybersecurity contributes to *hifz al-mal* (wealth protection) by preventing fund theft and unauthorized access, *hifz al-nafs* (soul protection) by providing peace of mind in transactions, and *hifz al-'aql* (intellect protection) by preventing fraud and confusion resulting from non-transparent information ((Hutagalung et al., 2025; Zulika et al., 2025).

Research on maqashid al-sharia in cybersecurity protection policies demonstrates that integrating maqashid al-sharia principles prioritizes not only technical aspects but also moral and social dimensions, thereby protecting consumer rights and maintaining justice in digital

transactions. (Rofiullah, 2025). Maqashid al-sharia provides a comprehensive framework for evaluating the extent to which cybersecurity policies not only protect customers' material assets but also provide psychological tranquility and empower customers through knowledge. (Kurnia et al., 2025; Sarpini, 2025). This framework also encompasses the aspects of *amanah* (trust) and *maslahah* (public good), whereby Islamic banks have the obligation to maintain customer trust in the management of funds and personal data. (Hutagalung et al., 2025; Zulika et al., 2025).

Four research gaps require addressing. First, a theoretical gap: no study has specifically linked technical cybersecurity implementation with maqashid al-sharia dimensions operationally within the context of Indonesian Islamic banking (Rofiullah, 2025; Hutagalung et al., 2025). Previous studies remain partial, with technical aspects discussed separately from the maqashid framework. (Kurnia et al., 2025; Sarpini, 2025). Second, an empirical gap: studies on cybersecurity in digital banking applications remain dominated by technical approaches and risk perception, without considering the maqashid al-sharia framework as an analytical lens (Putri et al., 2025; Utami, 2026). Third, a methodological gap: research remains dominated by quantitative approaches, while in-depth exploration of stakeholder meaning and experience regarding cybersecurity within the maqashid framework remains limited (Supriadi et al., 2025; Zulika et al., 2025). Fourth, a contextual gap: studies on Bank Muamalat DIN as a pioneer of digital Islamic banking in Indonesia have not been extensively conducted from a maqashid al-sharia perspective (Kurnia et al., 2025; Rofiullah, 2025).

Based on these gaps, this research is formulated around the main question: "How is cybersecurity implemented in Bank Muamalat's digital services from a maqashid al-sharia perspective?" elaborated through four sub-questions: (1) What cybersecurity infrastructure and policies are implemented in Muamalat DIN? (2) To what extent does cybersecurity implementation align with maqashid al-sharia principles (*hifz al-mal, al-nafs, al-'aql*)? (3) How does Bank Muamalat comply with cybersecurity regulations and Sharia fatwas? (4) How do customers perceive Muamalat DIN's cybersecurity in relation to maslahah?

This study aims to analyze the implementation of cybersecurity in Bank Muamalat's digital services from a maqashid al-sharia perspective. Specifically, it seeks to identify cybersecurity infrastructure and policies, analyze their alignment with maqashid al-sharia principles, evaluate compliance with regulations and sharia fatwas, and explore customer perceptions of Muamalat DIN's cybersecurity in relation to maslahah. This research is expected to provide a theoretical contribution by developing a maqashid al-sharia-based cybersecurity evaluation framework, a practical contribution through policy recommendations for Bank Muamalat and regulators, and a methodological contribution through maqashid-based interview and observation instruments (Rofiullah, 2025; Kurnia et al., 2025; Hutagalung et al., 2025; Maulia et al., 2025; Supriadi et al., 2025; Zulika et al., 2025).

This study references relevant previous research. Hutagalung et al., (2025) found that cybersecurity protection behavior reflects the principles of *hifz al-mal* and *amanah*, as described

by Protection Motivation Theory, yet does not address technical implementation from an institutional perspective. Putri et al., (2025) examined the role of cybersecurity software in maintaining customer trust at BSI, but did not employ the maqashid framework. Utami (2026) revealed that risk perception and data security influence Generation Z customer trust, yet focused on a single generation. Zulika et al., (2025) demonstrated that maslahah-based mobile banking positively influences customer loyalty, but did not specifically address cybersecurity aspects.

Rofiullah (2025) discussed the maqashid al-sharia framework in the digital economy broadly without empirical case studies. Kurnia et al., (2025) measured Islamic bank performance using the Maqashid Sharia Index without addressing cybersecurity. Maulia et al., (2025) found that service digitalization and the suitability of Sharia products positively influence customer satisfaction. Supriadi et al., (2025) examined Islamic banking digitalization in enhancing customer trust without employing the maqashid framework. Sarpini (2025) discussed Islamic economic transformation in the digital era, focusing on fintech and financial inclusion. Based on this literature review, a gap remains in the empirical integration of technical cybersecurity implementation with maqashid al-sharia principles in the Bank Muamalat DIN case study.

METHOD

This study employs a qualitative approach with an instrumental case study design to comprehensively understand cybersecurity implementation at Bank Muamalat and its relationship with maqashid al-sharia. (Creswell & Poth, 2018; Yin, 2018). The qualitative approach was selected for its ability to explore phenomena holistically and in context, capturing the meanings ascribed by various stakeholders to cybersecurity policies and practices. (Merriam & Tisdell, 2016; Denzin, 2018). The instrumental case study design enables researchers to understand the specific case (Muamalat DIN) while providing insights into the broader phenomenon of cybersecurity implementation in Islamic banking. (Stake, 1995).

Sampling

The target population comprises all stakeholders involved in implementing and using Bank Muamalat's digital services, particularly the Muamalat DIN application. The research context encompasses Indonesia's Islamic digital banking ecosystem, with a focus on Bank Muamalat Indonesia, the nation's first Islamic bank (Bank Muamalat Indonesia, 2024; Bank Muamalat Indonesia, 2025). The study was conducted at Bank Muamalat Genteng Banyuwangi Branch from January to June 2026. This location was selected based on Banyuwangi's significant economic growth and an active Islamic banking customer base, with the Genteng Branch serving as a hub for Islamic banking services in eastern East Java (Bank Muamalat Indonesia, 2025). This location enables capture of stakeholder perspectives at the branch level with diverse customer characteristics, ranging from farmers and fishermen to SMEs and professionals (Maulia et al., 2025). Informants were selected using purposive and snowball sampling techniques (Patton,

2015; Creswell & Poth, 2018). Informants comprise three groups with the following criteria: Active Muamalat DIN Customers (5 individuals), Bank Muamalat Management (2 individuals), and Bank Muamalat Sharia Supervisory Board (DPS) (1 individual).

Data collection employed three methods for comprehensive data triangulation (Denzin, 2018; Creswell & Poth, 2018):

1. In-depth Semi-structured Interviews using interview guidelines based on the maqashid al-sharia framework and cybersecurity indicators (Merriam & Tisdell, 2016; Patton, 2015). The interview guide encompasses four dimensions: (1) cybersecurity infrastructure and policies (encryption, authentication, timeout, education); (2) alignment with maqashid al-sharia (*hifz al-mal, al-nafs, al-'aql*); (3) regulatory and fatwa compliance (POJK No. 21/2023, DSN-MUI Fatwa No. 117/2018, DPS role) (OJK, 2023; Fatwa No. 117/DSN-MUI/II/2018 Tentang Layanan Keuangan Digital Syariah, 2018(4) customer perceptions (trust, experience, risk understanding, masalah contribution). Interviews were conducted face-to-face, lasting 60-90 minutes, recorded, and transcribed verbatim. (Creswell & Poth, 2018).
2. Direct Observation of the Muamalat DIN application interface and security procedures (Yin, 2018; Stake, 1995). Observed aspects include: security features (biometric login, notifications, encryption indicators, timeouts), security information (privacy policies, guidelines), customer education (articles, tutorials), and user experience (accessibility, clarity of instructions).
3. Documentation. Document collection includes: Bank Muamalat Annual Reports 2023-2024 (Bank Muamalat Indonesia, 2024; Bank Muamalat Indonesia, 2025), POJK No. 21/2023 (OJK, 2023), DSN-MUI Fatwa No. 117/2018 (D. S. N.-M. U. Indonesia, 2018)..

Data analysis employed Miles and Huberman's interactive model (2020), comprising three concurrent flows of activity. (Miles et al., 2020):

1. Data Reduction. Interview transcripts, observation notes, and documents were selected, focused, simplified, and abstracted.
2. Data Display. Data were presented in descriptive narratives, tables, and matrices to facilitate comprehension.
3. Verification and Conclusion Drawing. Conclusions were drawn progressively through verification via thematic patterns, cross-confirmation across sources and methods, member checking, and peer review.

RESULT AND DISCUSSION

1. Cybersecurity Infrastructure and Policies of Muamalat DIN

Based on interviews with Bank Muamalat's IT Manager (Informant M1) and direct observation of the Muamalat DIN application, Bank Muamalat has implemented a comprehensive cybersecurity infrastructure, including SSL 2048-bit encryption, biometric login,

two-factor authentication, and 5-minute timeout sessions (B. M. Indonesia, 2025). This finding aligns with Hutagalung et al., (2025), who emphasized the importance of layered protection in Islamic banking security systems. The bank actively educates customers through articles on cybercrime methods, such as phishing and social engineering. (Bank Muamalat Indonesia, 2024). Nurahmani (2026) adds that cyber threats in Islamic banking are increasingly complex with the emergence of Shadow AI, necessitating maqashid al-sharia-based digital governance.

Critical analysis reveals several considerations: (1) dependence on customer devices for biometric features presents a potential vulnerability. (Utami, 2026)(2) education remains predominantly text-based, yet to utilize interactive video tutorials (Maulia et al., 2025); and (3) no implementation of real-time AI-based threat detection systems (Sarpini, 2025). This aligns with Divia (2026) Findings indicate that technical constraints, such as login failures and system errors, persist in Muamalat DIN usage, diminishing the quality of the user experience.

2. Analysis of Cybersecurity Alignment with Maqashid al-Sharia Principles

a. Hifz al-Mal (Wealth Protection)

The implementation of cybersecurity in Muamalat DIN directly supports the principle of *hifz al-mal*. Allah SWT states in QS. An-Nisa verse 29: *"Do not kill yourselves. Indeed, Allah is ever Merciful to you."* Ibn 'Ashur, in his interpretation of at-Tahrîr wat Tanwîr, explains that this verse prohibits acts of self-destruction and destruction of property, as both contain elements of *itlaf* (source of damage). Protecting wealth from theft through encryption and layered authentication represents implementation of the prohibition against squandering wealth, as stated in the hadith narrated by Bukhari: *"Indeed, Allah dislikes three things: argumentation, squandering wealth, and excessive questioning"* (Al-Bukhari, n.d. No.1477).

The SSL 2048-bit encryption system and two-factor authentication prevent unauthorized access to customer accounts, protecting funds from theft. (B. M. Indonesia, 2025). The timeout session feature provides additional protection if customers leave devices unlocked. This finding aligns with Hutagalung et al., (2025), demonstrating that cybersecurity protection behavior reflects the principles of *hifz al-mal* and *amanah*, with their research model explaining 69.6% of the variance in cybersecurity protection behavior.

b. Hifz al-Nafs (Soul Protection)

Cybersecurity contributes to *hifz al-nafs* by fostering psychological peace of mind during transactions. Muamalat DIN's active user growth reached 673 thousand (18% YoY) with 7.7 million transactions (30% YoY) in Q1 2025 (Bank Muamalat Indonesia, 2025). QS. Al-Maidah verse 90 prohibits acts that destroy intellect and soul: *"O you who have believed, indeed, intoxicants, gambling, [sacrificing on] stone altars [to other than Allah], and divining arrows are but defilement from the work of Satan, so avoid it..."* (QS. Al-Maidah: 90). Sheikh Al-Thabary in Tafsir Al-Thabary explains that this verse prohibits Muslims from acts that destroy intellect and soul. Transaction comfort and security in digital transactions constitute part of soul protection from stress and financial loss. Customer N1 stated: *"I feel at ease using Muamalat DIN because there*

are notifications for every transaction and complete security features" (Interview, 2026). (2025) confirm that masalah-based mobile banking positively influences customer loyalty.

c. *Hifz al-'Aql* (Intellect Protection)

Information transparency and cybersecurity education are essential parts of *hifz al-'aql*. Bank Muamalat provides clear product information, education on fraud methods, and guidance on avoiding phishing. (Bank Muamalat Indonesia, 2024). QS. Al-An'am verse 152 emphasizes protection of wealth for those with weak intellect: *"And do not approach the orphan's property except in a way that is best [to improve it], until he reaches maturity"*. This verse teaches that wealth must be protected from damage, including through education, so customers are not deceived by misleading information. Bank Muamalat explicitly states that it never requests customer confidential data via telephone, SMS, or social media, protecting customers from confusion and fraud. (Bank Muamalat Indonesia, 2025). Obaid (2026) emphasizes that cybersecurity governance and robust digital systems are prerequisites for fintech integration and institutional resilience in Islamic banking.

Building on this foundation, the discussion of *hifz al-'aql* (protection of intellect) can be further expanded by proposing specific interactive educational strategies to address the intergenerational literacy gap identified in the interviews. Different age groups have varying levels of digital literacy and different preferences for information access, necessitating a multi-channel, interactive approach to ensure that intellectual protection reaches all customer segments effectively.

3. Compliance with Regulations and Sharia Fatwas

Bank Muamalat demonstrates compliance with POJK No. 21 of 2023 concerning Digital Services by Commercial Banks and DSN-MUI Fatwa No. 117/2018 concerning Information Technology-Based Financing Services. (OJK, 2023; Fatwa No. 117/DSN-MUI/II/2018 Tentang Layanan Keuangan Digital Syariah, 2018). The Sharia Supervisory Board (DPS) plays an active role in supervising sharia compliance, including security aspects that must uphold Islamic values. (Kurnia et al., 2025). Muamalat DIN also provides Islamic features such as zakat calculators, qibla direction, and Hijrah Amal features (zakat, infaq, sadaqah, waqf), with 1.1 million ZIS transactions by May 2025 (Bank Muamalat Indonesia, 2025). This demonstrates that digital services are not solely economically oriented but also fulfill customers' spiritual needs. (Maulia et al., 2025).

In Islamic Economic Law, cybersecurity falls within the domain of muamalah and is permissible, and even obligatory, to implement as a preventive measure against harm. The fiqh principle states: *"Fundamentally, all forms of muamalah are permissible unless there is evidence prohibiting them"* (Antasari, 2023). The basis for this principle is QS—Al-Maidah verse 87, which prohibits forbidding what is lawful and transgressing boundaries. Cybersecurity in digital banking is permissible, as it provides benefits and protection, provided it contains no prohibited substance elements, prohibited non-substance elements, or invalid contracts (Antasari, 2023).

Nurahmani (2026) adds that Shadow AI, as an operational risk source, requires a maqashid al-sharia-based governance framework to manage sharia compliance, cyber, and reputational risks.

The DPS's active role in overseeing Muamalat DIN's sharia compliance reflects the implementation of the principles of *amanah* and *maslahah* in bank operations. (Hutagalung et al., 2025; Zulika et al., 2025). This is important because in the Islamic banking context, sharia compliance is not merely a formal obligation but also the foundation of customer trust. (Supriadi et al., 2025). Maulia et al., (2025) found that product alignment with Sharia principles positively influences customer satisfaction, thereby enhancing loyalty and trust.

However, critical analysis indicates that compliance with regulations and Sharia fatwas has not been fully integrated into cybersecurity policies. Despite DPS involvement in supervision, no specific framework directly links cybersecurity indicators to maqashid al-sharia dimensions in formal bank policies. (Rofiullah, 2025; Kurnia et al., 2025). This aligns with Sarpini, (2025) Findings that integrating Sharia values into financial technology still require developing a more systematic and measurable framework. Obaid (2026) emphasizes that cybersecurity governance and robust digital systems are prerequisites for fintech integration and institutional resilience in Islamic banking. This research recommends that Islamic banks develop cybersecurity risk management frameworks integrated with sharia compliance to address increasingly complex challenges in the digital era.

4. Customer Perceptions and Maslahah

Customers demonstrated high trust levels with a satisfaction score of 82.22% (Bank Muamalat Indonesia, 2025). Customer N3 stated: *"Initially, I was hesitant about digital transactions, but after the security features were explained and there was education, I became confident"* (Interview, 2026). Maslahah perceived by customers encompasses wealth protection, peace of mind, and convenient access to services. Sasmita (2024) affirms that Islam teaches protection and respect for human rights by safeguarding five fundamental rights: freedom, life, equality, wealth protection, and justice.

However, intergenerational literacy gaps remain challenging. Senior customer (N5) stated: *"I still lack understanding of digital security; the bank should provide more direct socialization"* (Interview, 2026). This aligns with Utami (2026), who found generational differences in risk perception. Divia (2026) Research also identified non-technical constraints, such as low digital literacy and limited social interaction, which reinforced perceptions of difficulty using the service. However, dimensions of responsiveness, assurance, and empathy are maintained through the active role of bank staff.

Comparison with Previous Research

This research strengthens Hutagalung et al., (2025) Findings on cybersecurity behavior as a reflection of Hifz al-Mal, while extending them by demonstrating the implementation of three maqashid dimensions simultaneously. This research also complements Putri et al., (2025) and

Utami (2026) Findings demonstrate that cybersecurity influences trust through fulfillment of maqashid al-sharia values. The novel contribution of this research is the identification of intergenerational cybersecurity literacy gaps and the development of a maqashid al-sharia-based cybersecurity evaluation framework addressing the theoretical gap identified by Rofiullah (2025). Nurahmani (2026) and Obaid (2026) Reinforce the urgency of maqashid-based cybersecurity governance in addressing increasingly complex and sophisticated cyber threats in the digital era.

CONCLUSION

This study concludes that the implementation of cybersecurity in Muamalat DIN comprehensively reflects the maqashid al-sharia principles across three primary dimensions. First, cybersecurity implementation, including 2048-bit SSL encryption, two-factor authentication, biometrics, and session timeouts, supports *hifz al-mal* (wealth protection) by preventing unauthorized access and the theft of customer funds. This aligns with QS. An-Nisa verse 29, which prohibits acts damaging wealth and soul, and the hadith narrated by Bukhari prohibiting squandering wealth.

Second, cybersecurity contributes to *hifz al-nafs* (soul protection) by fostering psychological peace of mind during transactions, as reflected in the growth of active users. This implements QS—Al-Maidah verse 90, which prohibits acts that destroy the intellect and soul. Third, information transparency and cybersecurity education provided by Bank Muamalat constitute the implementation of *hifz al-'aql* (intellect protection), protecting customers from confusion and fraudulent information, aligning with QS—al-An'am verse 152, which teaches protecting wealth for those with weak intellect. Bank Muamalat demonstrates compliance with POJK No. 21 of 2023 and DSN-MUI Fatwa No. 117/2018 through active DPS supervision and provision of Islamic features (zakat calculator, qibla direction, Hijrah Amal). From the perspective of Islamic Economic Law, cybersecurity falls within muamalah that is permissible and even obligatory as a preventive measure against harm, consistent with the fiqh principle that all forms of muamalah are permissible unless evidence prohibits them.

Customer perceptions of Muamalat DIN cybersecurity are positive, yet intergenerational literacy gaps persist, particularly among senior customers who require support. The urgency of cybersecurity in realizing *maslahah* is paramount as it protects assets, provides psychological peace, and empowers customers through knowledge. Cybersecurity failure can destroy trust and undermine customer well-being, contradicting Sharia objectives.

Recommendations for future research: Conduct comparative studies across Islamic banks in Indonesia to map maqashid-based cybersecurity standards and identify best practices that can be adopted by other Islamic banks, including comparisons with Islamic banks in other countries such as Malaysia and the Middle East.

REFERENCES

- Al-Bukhari, I. (n.d.). *Shahih al-Bukhari*.
- Antasari, U. I. N. (2023). *Cyber Security dalam Hukum Ekonomi Syariah*. UIN Antasari.
- Creswell, J. W., & Poth, C. N. (2018). *Qualitative Inquiry and Research Design: Choosing Among Five Approaches (4th ed.)*. Sage Publications.
- Denzin, N. K. (2018). *The qualitative manifesto: A call to arms*. Routledge.
- Divia. (2026). *Analisis Kualitas Layanan Aplikasi Muamalat DIN*.
- Fatwa No. 117/DSN-MUI/II/2018 tentang Layanan Keuangan Digital Syariah (2018).
- Hutagalung, M. W. R., Siregar, S., Furqan, M., Pulungan, I., & Elce, F. (2025). Cybersecurity Behavior as a Reflection of Ḥifẓ al-Māl in Islamic Banking: A Behavioral Model Based on Protection Motivation Theory. *El-Qist: Journal of Islamic Economics and Business (JIEB)*, 15(2), 127–153. <https://doi.org/10.15642/elqist.2025.15.2.127-153>
- Indonesia, Bank Muamalat (2024). *Laporan Tahunan Bank Muamalat Indonesia 2023*. Bank Muamalat Indonesia.
- Indonesia, Bank Muamalat (2025). *Laporan Tahunan Bank Muamalat Indonesia 2024*. Bank Muamalat Indonesia. <https://www.bankmuamalat.co.id>
- Indonesia, D. S. N.-M. U. (2018). *Fatwa DSN-MUI Nomor 117/DSN-MUI/II/2018 tentang Layanan Pembiayaan Berbasis Teknologi Informasi Berdasarkan Prinsip Syariah*. DSN-MUI.
- Kurnia, N., Wartoyo, & Bakhri, S. (2025). Analisis Komparasi Kinerja Bank Umum Syariah di Indonesia Menggunakan Maqashid Sharia Index. *Velocity: Journal of Sharia Finance and Banking*, 5(1).
- Maulia, N., Afif, Y. K., Putri, R. A., Mayori, E. R., & Salsabila, S. (2025). The Role of Service Digitalization and Sharia Product Suitability in Bank Customer Satisfaction. *Mudharib: Jurnal Ekonomi Dan Keuangan Syariah*, 6(3).
- Merriam, S. B., & Tisdell, E. J. (2016). *Qualitative Research: A Guide to Design and Implementation (4th ed.)*. Jossey-Bass.
- Miles, M. B., Huberman, A. M., & Saldaña, J. (2020). *Qualitative data analysis: A methods sourcebook (4th ed.)*. SAGE Publications.
- Nurahmani, R. (2026). Shadow AI: Ancaman Baru bagi Tata Kelola Perbankan Syariah. *Jurnal Manajemen Risiko Perbankan Syariah*.
- Obaid, A. (2026). Cybersecurity Governance and Institutional Resilience in Islamic Banking. *International Journal of Islamic Finance*.
- OJK. (2023). *Cetak biru pengembangan dan penguatan perbankan syariah Indonesia 2023–2027*. Otoritas Jasa Keuangan.
- Patton, M. Q. (2015). *Qualitative Research & Evaluation Methods: Integrating Theory and Practice (4th ed.)*. Sage Publications.
- Putri, D. A., Aisyah, N., Febrian, S., & Nurbaiti. (2025). Peran Software Cyber Security dalam Menjaga Kepercayaan Nasabah pada Transaksi Digital di BSI. *International Journal of Islamic Business Management (IJMBS)*, 4(4), 52–56.
- Rofiullah, A. H. (2025). Pengembangan Ekonomi Syariah dalam Perspektif Maqashid Syariah di Era Ekonomi Digital. *SAUJANA: Jurnal Perbankan Syariah Dan Ekonomi Syariah*, 7(2), 24–43.
- Sarpini, S. (2025). The Transformation of Islamic Economics in The Digital Era: An Analysis of Islamic Fintech and Financial Inclusion in Indonesia. *Ijtima'iyya: Jurnal Pengembangan Masyarakat Islam*, 10(1).

- Sasmita. (2024). Perlindungan Hak Asasi Manusia dalam Perspektif Maqashid Syariah. *Jurnal Hukum Ekonomi Syariah*.
- Stake, R. E. (1995). *The Art of Case Study Research*. Sage Publications.
- Supriadi, Z. S., & Rafif, M. S. (2025). Digitalisasi Perbankan Syariah dalam Meningkatkan Kepercayaan Nasabah Bank Syariah Indonesia (BSI) KC Makassar. *Al-Zayn: Jurnal Ilmu Sosial & Hukum*, 3(6), 8371–8383.
- Utami, K. (2026). Pengaruh Persepsi Risiko, Keamanan Data, dan Transparansi terhadap Kepercayaan Nasabah Generasi Z pada Layanan Digital Bank Syariah di Kabupaten Sumenep. *JES (Jurnal Ekonomi Syariah)*, 11(1), 1–10.
- Yin, R. K. (2018). *Case Study Research and Applications: Design and Methods (6th ed.)*. Sage Publications.
- Zulika, Z., Misbach, I., Sapa, N. B., Irawan, H., & Qubais, M. A. (2025). User Interest in Masalahah-Based Mobile Banking for Maintaining Customer Loyalty. *Finansia: Jurnal Akuntansi Dan Perbankan Syariah*, 8(2).