Journal of Business Management and Islamic Banking
E-ISSN: 2694-2787
Vol. 5, No. 1, 2026
pp.77-94
DOI: https://doi.org/10.14421/jbmib.2026.0501-05

Maqasid Al Shariah Framework for Cybersecurity Risk Management and Data Protection in Global Islamic Banking

Bintang Junita[1] , Muhammad Senoyodha Brennaf [2] , Dicky Octaviano[1]*, Zulfati Dinul Fatiha[3]

[1]Faculty of Economics and Business, Universitas Bina Sarana Informatika, Jakarta, Indonesia
[2]University of Sheffield, Sheffield S1 4DP, United Kingdom
[3]Faculty of Information Technology, Universitas Bina Sarana Informatika, Jakarta, Indonesia

*Corresponding author: dicky.doc@bsi.ac.id

Article History
Received : 2026-04-11
Revised : 2026-04-16
Accepted : 2026-06-20

Abstract

Purpose— This study investigates the influence of cybersecurity risk management and data protection governance on Islamic Financial Institutions (IFIs) through the lens of *Maqasid Al Shariah*. As IFIs accelerate digitalisation, safeguarding the ummah's financial and personal data has become both a Shariah imperative and a strategic priority. Variables examined include regulatory framework maturity, Shariah governance integration, incident management capacity, data protection mechanisms, and AI governance across five major jurisdictions.

Design/methodology/approach— A qualitative comparative analysis (QCA) is employed across Malaysia, the UAE, Saudi Arabia, Indonesia, and the United Kingdom. Secondary data encompass regulatory publications (2019–2024), IFI annual reports, IFSB GN 6 (2021) standards, and global cybersecurity incident databases from IBM, IMF, and Interpol.

Findings— Significant jurisdictional heterogeneity in cybersecurity maturity is revealed. Malaysia (Maqasid Alignment Score/MAS: 4.4) and the UK (MAS: 4.0) exhibit the strongest Maqasid alignment, while Indonesia (MAS: 3.1) and Saudi Arabia (MAS: 3.5) show emerging profiles. A critical universal gap is identified: no jurisdiction formally mandates Shariah Supervisory Board (SSB) engagement in technology risk governance.

Research implication/limitation—The analysis is confined to five jurisdictions and qualitative comparative data. Future studies should apply quantitative methods and extend to additional markets. Results offer actionable guidance for regulators, Shariah boards, and IFI management in formulating cybersecurity strategies aligned with Islamic ethical obligations.

Originality/value—This study constructs the first systematic Maqasid cybersecurity mapping matrix applicable to global IFIs, bridging classical Islamic jurisprudence and contemporary digital governance scholarship, and explicitly compared with established secular frameworks National Institute of Standards and Technology Cybersecurity Framework (NIST CSF) 2.0, ISO/IEC 27001:2022, and Control Objectives for Information and Related Technologies (COBIT) 2019.

Keywords: Cybersecurity, *Maqasid Al Shariah*, Islamic Banking, Data Protection, Risk Management
JEL Classifications: G21, G28, G32, Z12

This is an open-access article under the CC BY-NC license.
How to cite: Junita et al. (2026). Maqasid Al Shariah Framework for Cybersecurity Risk Management and Data Protection in Global Islamic Banking *Journal of Business Management and Islamic Banking*, *5*(1),077-094. https://doi.org/10.14421/jbmib.2026.0501-05.

1. Introduction

The rapid digitalisation of global financial services has fundamentally transformed the operational landscape of Islamic banking. Islamic Financial Institutions (IFIs), including full-fledged Islamic banks, Islamic windows of conventional banks, and Islamic microfinance institutions, are increasingly deploying mobile banking platforms, artificial intelligence (AI) driven credit scoring systems, blockchain-based sukuk settlement infrastructure, open banking application programming interfaces (APIs), and cloud-hosted core banking solutions. World Bank (2023) documented that Islamic banking digitalisation grew at a compound annual growth rate (CAGR) of 24% between 2018 and 2022, significantly outpacing conventional banking digitisation in emerging markets. The Islamic Financial Services Board (IFSB, 2024) further reported that over 67% of IFIs globally had launched dedicated mobile banking platforms by the end of 2023. PwC's Global FinTech Report (2023) identified AI adoption as a core strategic priority for 77% of financial institutions worldwide. While these advances expand financial inclusion and enhance service efficiency, they simultaneously expose IFIs and their customers to unprecedented cybersecurity risks. For Islamic banks, digital vulnerability is not merely a technical concern; it constitutes a profound ethical obligation grounded in the classical Islamic principle of *la darar wa la dirar* (no harm shall be inflicted or reciprocated) (Al-Nawawi, 1900).

The scale of global cyber threats targeting the financial sector has intensified dramatically. The International Monetary Fund (IMF, 2024) documented cumulative cyber losses exceeding USD 12 billion between 2004 and 2023. Corroborating this trend, Deloitte's Global Cyber Risk Report (2023) identified financial services as the most targeted industry globally for the fourth consecutive year, with a 38% year on year increase in sophisticated attacks on banking infrastructure. Consistent with these findings, Batista (2023) demonstrated in a longitudinal study of 124 financial institutions across 34 countries that cyber incident frequency in banking increased at 2.8 times the rate of other sectors between 2019 and 2023, with emerging market Islamic banks exhibiting the steepest growth trajectory. IBM Security (2023) recorded the global average cost per breach at USD 4.45 million, an all-time high, while financial services accounted for 18.3% of all reported incidents in 2023. Ransomware attacks against financial institutions increased by 62% between 2020 and 2023 (Interpol, 2023).

Islamic banks, which collectively managed assets exceeding USD 4.0 trillion as of 2024 (IFSB, 2024), represent an increasingly distinctive target. This study focuses on five jurisdictions Malaysia, the UAE, Saudi Arabia, Indonesia, and the United Kingdom which together account for approximately 78% of global Islamic banking assets (IFSB, 2024) and represent the full spectrum of Islamic banking governance models: Muslim majority markets with dedicated Islamic banking legislation (Malaysia, Saudi Arabia, Indonesia), a hybrid global Islamic financial hub (UAE), and a non Muslim majority market hosting significant Islamic banking operations under a conventional regulatory framework (UK). This multi-model selection ensures the findings are generalisable beyond any single jurisdiction and capture the structural diversity of global Islamic banking governance. IFIs face a compounded cybersecurity challenge: dual compliance under secular financial regulation and Shariah governance creates oversight structures with potential gaps in emerging domains such as cybersecurity (Grassa & Matoussi, 2014). The global Islamic FinTech sector

further amplifies this challenge: IFN FinTech (2023) reported USD 6.7 billion in Islamic FinTech investments in 2023 across 450+ active startups in 30 countries, each representing a potential vulnerability in the wider IFI ecosystem.

The gravity of these risks was vividly illustrated in May 2023, when Bank Syariah Indonesia (BSI) formed through the merger of BRI Syariah, BNI Syariah, and Bank Syariah Mandiri in 2021 Qibtiyah & Wicaksono (2022) suffered a ransomware attack attributed to LockBit 3.0, compromising approximately 15 million customer records and disrupting ATM and mobile banking services for approximately five days during Eid al-Fitr (Ahmarani et al., 2025). From the Maqasid Al Shariah perspective, this incident simultaneously violated *hifz al mal* (access to wealth), *hifz al nafs* (welfare during a sacred period), and *hifz al aql* (integrity of financial information) a multi-dimensional harm taxonomy illustrating both the analytical utility of the Maqasid framework and the inadequacy of current governance structures.

Despite the evident urgency, the academic literature remains sparse in addressing cybersecurity through Islamic jurisprudence. Extant scholarship focuses on credit risk (Mishkin & Eakins, 2021), operational risk, and Shariah non-compliance risk (Fasa, 2020), while cybersecurity governance remains peripheral. Found that Islamic banks in the MENA region exhibit significantly lower cybersecurity disclosure transparency than conventional counterparts, attributing this gap to the absence of Shariah-based cybersecurity reporting standards. Documented that regulatory fragmentation across Islamic banking jurisdictions creates exploitable governance inconsistencies, a structural vulnerability directly addressed by this study's comparative approach. The IFSB Guidance Note GN 6 (2021) is the most authoritative Shariah-sensitive cybersecurity guidance but lacks binding force and stops short of articulating an explicit Maqasid framework for digital risk governance (Hassan & Lewis, 2007).

The concept of *amanah* (trustworthiness and stewardship) is foundational to Islamic commercial ethics. An Islamic bank failing to invest adequately in cybersecurity has breached the amanah relationship that legitimises its existence as an Islamic institution (Kamali, 2012). Demonstrated that Islamic banking digital platforms are disproportionately vulnerable to social engineering attacks precisely because trust-based customer relationships central to Islamic finance are actively exploited by cybercriminals who impersonate Shariah advisors and bank representatives. This finding underscores that the communitarian ethos of Islamic finance, far from being merely a normative principle, has direct operational cybersecurity implications.

The macroeconomic environment also influences IFI's cybersecurity investment capacity. Mamuaja et al., (2024) demonstrated that money supply expansion and economic growth create conditions for increased banking digitalisation, thereby expanding cybersecurity exposure, while Mutmainah et al., (2024) showed that monetary policy transmission through Islamic banking channels increasingly depends on the resilience of digital payment infrastructure. This macroeconomic dimension confirms that cybersecurity is not merely an internal governance issue for individual IFIs but a systemic concern for Islamic financial system stability (Pamungkas et al., 2025).

Prior studies on Islamic banking governance have applied Maqasid Al Shariah to financial product permissibility (Dusuki & Abdullah, 2007), corporate social responsibility

(Kamali, 2012), and sustainable finance (Hasan & Asutay, 2011). However, no one has constructed a systematic mapping between Maqasid dimensions and cybersecurity governance domains, nor proposed a quantifiable, replicable Maqasid Alignment Score for cross-jurisdictional benchmarking. This study's novelty rests on three specific contributions absent from all prior scholarship: (1) the first operationalisation of all five classical Maqasid extended with *hifz al bi'ah* (Kamali, 2025) as a structured cybersecurity governance evaluation framework; (2) the construction of a scored MAS instrument enabling comparative governance assessment across jurisdictions; and (3) a systematic five jurisdiction QCA comparison using verifiable regulatory and institutional evidence covering the 2019–2024 period.

Building on this context, this study advances a *Maqasid Al Shariah-grounded* framework for cybersecurity risk management and data protection, applying it comparatively across five major jurisdictions. The findings provide theoretical contributions to Islamic economics literature and practical guidance for regulators, Shariah board members, and IFI management in formulating cybersecurity strategies adaptive to Shariah obligations.

2. Literature Review

2.1 Cybersecurity in Islamic Financial Institutions

Alharbi et al., (2024) examined operational risk in Islamic banks across GCC countries and found that technology risk was the fastest-growing risk category between 2019 and 2023, with a compound annual growth rate (CAGR) of 34% in reported incidents. Nouman et al., (2022) demonstrated that while Islamic banks employ interest-free instruments, their structural exposure to technology-mediated risk is equivalent to conventional banks, with additional Shariah compliance monitoring systems creating unique attack surfaces. The IFSB's GN 6 (2021) represents the most authoritative Shariah-sensitive cybersecurity guidance, but lacks binding force, and secular frameworks, NIST CSF 2.0, and ISO/IEC 27001:2022 are ethically neutral, incapable of capturing the normative obligations Islamic banks owe the ummah (Chapra, 2008).

Expanding the empirical base with more recent Scopus-indexed studies: Lassoued (2022) identified significantly lower cybersecurity disclosure transparency in MENA Islamic banks, attributing this to absent Shariah based reporting standards. Alam et al., (2023) demonstrated that trust-based Islamic banking relationships create unique social engineering vulnerabilities, a form of hifz al aql breach. Hasan, et al., (2023) documented that regulatory fragmentation across Islamic banking jurisdictions creates exploitable governance inconsistencies. Zahroh et al., (2024) found that data governance maturity among Indonesian Islamic banks remains significantly below ASEAN peers. Arif et al., (2024) demonstrated that Malaysian IFIs achieving PDPA compliance exhibit 34% lower rates of data related regulatory sanctions, establishing a direct empirical linkage between data governance maturity and institutional performance.

The five constructs examined in this study each correspond to a distinct strand of cybersecurity governance scholarship. (1) Regulatory framework maturity has been extensively studied in conventional banking (Mishkin & Eakins, 2021) but is limited in IFI specific contexts (Grassa & Matoussi, 2014). (2) Shariah governance integration with

technology risk is uniquely relevant to IFIs; no prior study has examined SSB involvement in technology risk governance. (3) Incident management capacity addressed in operational resilience literature (IFSB GN 6, 2021; Batista, 2023). (4) Data protection mechanisms covered in privacy law scholarship (Malfiandri et al., 2025; Zahroh et al., 2024) but not mapped onto Maqasid dimensions. (5) AI governance standards in Islamic banking are an emerging field with no prior systematic treatment (Alam et al., 2023; Hasan et al., 2023). This multi-construct approach enables the MAS to evaluate governance comprehensiveness across all dimensions, rather than any single factor in isolation.

2.2 Maqasid Al Shariah as a Governance Framework

Maqasid Al Shariah was systematised by Al Ghazali (1993) in *Ihya Ulum al Din* and refined by Al Shatibi (2004) in *Al Muwafaqat*. The five Maqasid have been applied to banking products (Dusuki & Abdullah, 2007), corporate governance (Iqbal & Mirakhor, 2011), and sustainable finance (Hasan & Asutay, 2011b). However, their systematic application to digital governance remains largely unexplored. Fatoni & Sidiq (2019); Rahmatika & Romadhani (2021) argued that Shariah governance must extend to digital channels, while Anisak & Bakhri (2024) identified digital financial inclusion as a Maqasid objective implicitly requiring protective cybersecurity infrastructure. The present study constructs the first systematic Maqasid cybersecurity mapping matrix, validating it comparatively across five jurisdictions. Kamali (2025) has provided authoritative grounds for extending the classical five to include *hifz al bi'ah* (protection of the environment), recognising that *Khalifah* (stewardship of creation) is integral to *maqasid* fulfilment in the modern era. This sixth dimension, incorporated in Table 1 of this study, maps onto sustainable digital infrastructure governance, including green data centre operations and responsible data storage minimisation, an area of growing regulatory and societal importance not addressed by any prior Maqasid governance study.

2.3 Data Protection and Privacy in Islamic Finance

Data protection intersects with Islamic ethical imperatives around personal dignity (*karamah*) and privacy (*hishma*). Comprehensive legislation, Malaysia's Personal Data Protection Act (PDPA) 2010 (amended 2023) and Indonesia's UU PDP 2022, creates compliance obligations for IFIs, but as Malfiandri et al., (2025) observe, implementation capacity among smaller IFIs in developing markets lags behind legislative intent. Siregar et al., (2025) note that Islamic banks' monetary stability role means cybersecurity failures have macroprudential consequences. Mamuaja et al., (2024) further demonstrated that money supply expansion correlates with Islamic banking digitalisation, creating compounding cybersecurity exposure that demands governance frameworks sensitive to both macroeconomic dynamics and Shariah obligations.

2.4 Theoretical Framework

The analytical architecture of this study rests on the systematic mapping of the five Maqasid Al Shariah objectives onto modern cybersecurity domains. This framework

integrates three theoretical pillars: (1) Al Shatibi's *maqasid* theory from *Al Muwafaqat*; (2) the bank intermediation theory (Diamond, 1984a), positing that Islamic banks' custodial function over community wealth creates fiduciary data obligations; and (3) stakeholder theory (Freeman, 1984), adapted to encompass the ummah as a collective stakeholder whose digital interests Islamic banks must protect. The purchasing power theory Mankiw, (2019) also informs this framework: as digital assets increasingly represent a form of mal (wealth), the classical prohibition of harm to wealth extends directly to cybersecurity failures. The mapping in Table 1 was constructed through a three stage process: (1) systematic literature review identifying cybersecurity control categories from NIST CSF 2.0 (2024), ISO/IEC 27001:2022, and COBIT 2019; (2) deductive mapping of each control category to the corresponding Maqasid objective based on the Islamic jurisprudential principle most directly implicated, following the daruriyyat level primacy rule; and (3) validation against IFSB GN 6 (2021) to confirm alignment with existing Islamic financial regulatory standards. Where multiple Maqasid dimensions were implicated, the primary daruriyyat level Maqasid was applied. The mapping was not adapted from any prior governance maturity model; it is an original framework derived from the first principles integration of NIST, ISO, and Maqasid jurisprudence.

Table 1. Maqasid Al Shariah and Cybersecurity Risk Mapping Matrix

Maqasid Pillar	Arabic Term	Cybersecurity Dimension	Data Protection Relevance	Shariah Principle
Protection of Religion	*Hifz al Din*	Shariah compliance of AI/digital systems; prohibition of haram enabling technology; integrity of fatwa platforms	Ethical data monetisation policy; prohibition of data sharing enabling haram activities	Amanah; Ihsan; La Darar
Protection of Life	*Hifz al Nafs*	System availability (≥99.9% SLA); BCP/DRP; anti-Distributed Denial of Service (DDoS); physical security of data centres	Biometric data protection; identity theft prevention; customer safety	La darar wa la dirar
Protection of Intellect	*Hifz al Aql*	Data integrity; AI algorithmic fairness; explainable AI (XAI); anti misinformation in digital banking	Accuracy of financing records; right to explanation of algorithmic credit decisions	Haqq al Ilm; Sidq
Protection of Lineage	*Hifz al Nasl*	Customer Personally Identifiable Information (PII) privacy; family data protection; Know Your Customer (KYC) data hygiene; genetic/health data segregation	General Data Protection Regulation (GDPR)-equivalent PII protection; prohibition of family data sharing without explicit consent	Satr al Awrah; Hishma
Protection of Wealth	*Hifz al Mal*	End to end encryption; MFA; fraud detection; secure payment rails; HSM deployment	Secure custody of funds; anti theft systems; prohibition of electronic ghasb (misappropriation)	Prohibition of Riba, Gharar, Maysir

Maqasid Pillar	Arabic Term	Cybersecurity Dimension	Data Protection Relevance	Shariah Principle
Protection of Environment (Contemporary Extension)	*Hifz al Bi'ah*	Green data centre operations; energy efficient cloud infrastructure; digital carbon footprint minimisation; sustainable IT asset lifecycle management	Responsible data storage minimisation; prohibition of digital waste harming the environment; Shariah compliant data centre procurement	Khalifah; Mizan; La Fasad

Source (s): Authors' synthesis based on IFSB GN 6 (2021), Al Shatibi's Al Muwafaqat, NIST CSF 2.0 (2024), ISO/IEC 27001:2022

The mapping in Table 1 reveals analytically significant patterns. Hifz al mal commands the broadest correspondence with existing cybersecurity controls, reflecting Islamic banks' primary custodial function. Hifz al aql maps onto AI ethics and algorithmic explainability, increasingly critical as IFIs deploy machine learning for credit scoring (Mamuaja et al., 2024). Most innovatively, hifz al nasl provides jurisprudential grounding for GDPR equivalent personal data protection, framing privacy not as an imported Western construct but as an indigenous Shariah obligation. Hifz al din protection of religion maps onto the least discussed cybersecurity domain: the integrity of Shariah governance systems themselves, including AI-assisted Shariah compliance monitoring tools that could systematically misclassify transactions if compromised. Hifz al bi'ah, the sixth dimension, maps onto sustainable digital infrastructure governance, distinguishing the MAS from all existing governance maturity models (NIST CSF, CMMI, Gartner IT Score), which contain no environmental dimension for digital operations. This distinction represents a meaningful contribution to governance benchmarking scholarship

3. Methodology

This research employs Qualitative Comparative Analysis (QCA), a configurational comparative methodology developed by Ragin (1987) and extended by Schneider and Wagemann (2012), specifically designed for systematically comparing a small to medium number of cases (N = 5 to 50) across multiple conditions to identify causal configurations. This study employs crisp set QCA (csQCA) for three reasons: (1) the small number of jurisdictions (N = 5) precludes quantitative regression analysis; (2) the research question concerns combinations of governance conditions no single factor determines outcomes independently (Rihoux & Ragin, 2009; Fiss, 2011); and (3) csQCA is consistent with best practice for governance comparative research involving binary regulatory presence/absence indicators. The analysis was conducted through structured manual comparative scoring rather than dedicated QCA software (such as fs/QCA or R's QCA package), as csQCA calibration is appropriate for the binary indicators used and manual scoring ensures full auditability of each scoring decision (Permana & Ikasari, 2023).

The MAS was constructed as a five point composite index evaluating each jurisdiction across: (1) explicit legal instruments addressing each Maqasid dimension (0–1); (2) IFI specific regulatory guidance (0–1); (3) evidence of regulatory enforcement actions (0–1); (4) industry adoption rate exceeding 75% of major IFIs (0–1); and (5) formal SSB integration in technology risk oversight (0–1). Equal weighting was adopted as a conservative default,

consistent with governance index construction methodology Kaufmann, Kraay & Mastruzzi (2010), and standard practice in comparative governance research (Djankov et al., 2010). Expert validation was operationalised through inter-rater reliability assessment: two members of the research team independently scored all jurisdictions, achieving Krippendorff's alpha of 0.84, Hayes & Krippendorff (2007), indicating strong reliability. Subjectivity was minimised by grounding all scores exclusively in verifiable, publicly available documentary evidence, with no reliance on researcher judgement for indicator calibration. The MAS scoring rubric and all source documents are available from the corresponding author on request, supporting full replicability.

4. Results and Discussions

4.1 Comparative Regulatory Framework Analysis

Table 2 presents a cross-jurisdictional overview of cybersecurity governance frameworks. The analysis reveals substantive heterogeneity in regulatory sophistication, Shariah governance integration, and enforcement capacity across the five jurisdictions studied.

Table 2. Comparative Cybersecurity Governance Frameworks for Islamic Banks (2024)

Country / IFI	Regulatory Body	Key Cyber Framework	Maqasid Pillars Covered	Maturity Level
Malaysia (Maybank Islamic, CIMB Islamic)	Bank Negara Malaysia (BNM)	Risk Management in Technology (RMiT) 2020 (updated 2023), PDPA 2010 (amend. 2023), BNM Cyber Hygiene 2023	*Mal, Aql, Nafs, Din*	Advanced (MAS: 4.4)
UAE (ADIB, Dubai Islamic Bank)	Central Bank of the UAE (CBUAE), Abu Dhabi Global Market (ADGM), UAE IA	UAE Cyber Framework 2023, PDPL 2021, CBUAE Circular 28/2023	*Mal, Din, Nafs*	Advanced (MAS: 4.2)
Saudi Arabia (Al Rajhi Bank, Bank AlJazira)	Saudi Arabian Monetary Authority (SAMA), National Cybersecurity Authority (NCA)	ECC 1.0, NDMO, SAMA Cyber Framework 2023	*Mal, Din*	Developing (MAS: 3.5)
Indonesia (BSI, Bank Muamalat)	Otoritas Jasa Keuangan/Financial Services Authority of Indonesia (OJK), Bank Indonesia	POJK No. 11/2022, SEOJK 29/2022, UU PDP 2022	*Mal, Aql*	Emerging (MAS: 3.1)
United Kingdom (Al Rayan Bank,	Financial Conduct Authority (FCA), Prudential Regulation	UK GDPR,	*Mal, Nafs,*	Advanced (MAS: 4.0)

Country / IFI	Regulatory Body	Key Cyber Framework	Maqasid Pillars Covered	Maturity Level
Gatehouse Bank)	Authority (PRA), Information Commissioner's Office (ICO)	Cyber Essentials+, FCA SYSC 15A	*Nasl, Aql*	

Source(s) : BNM (2024), CBUAE (2023), SAMA (2023), OJK (2023), FCA/PRA (2024); Authors' compilation

Malaysia's MAS of 4.4 is explained by three institutional factors absent in other jurisdictions: (1) BNM mandates that technology risk be reported to the Board Risk Committee, creating governance accountability structurally analogous to Shariah board oversight an institutional arrangement that uniquely bridges secular IT governance and Shariah supervision; (2) Malaysia's dual regulatory mandate for both Islamic banking and financial technology has accelerated integration of cybersecurity into holistic governance frameworks; and (3) BNM's 2023 supervisory review found that 62% of Malaysian IFIs had voluntarily integrated RMiT compliance into their annual Shariah audit processes the highest cross pillar integration rate in the sample. Malaysia's four pillar coverage (*Mal, Aql, Nafs, Din*) reflects: RMiT encryption mandates (*Mal*); BNM 2023 AI ethics guidelines (*Aql*); mandatory BCPs with 4-hour RTO protecting service continuity (Nafs); and emerging SSB engagement (*Din*). This finding is supported by Lassoued (2022), who identified regulatory comprehensiveness as the primary predictor of cybersecurity maturity in Islamic banking contexts (Gartner, 2023). Saudi Arabia's MAS of 3.5 and two pillar coverage (*Mal, Din*) reflects a specific configuration: SAMA's strong financial encryption and fraud prevention mandates address hifz al mal comprehensively, and SAMA's Shariah compliance system integrity requirements address *hifz al din*. However, Saudi Arabia has no binding personal data privacy legislation equivalent to PDPA or GDPR (absence of *hifz al nasl* coverage), no published AI ethics guidelines for IFIs (absence of *hifz al aql*), and no mandatory BCP requirements for IFIs with tested RTOs (absence of *hifz al nafs*). SAMA's supervisory assessment (2023) found that only 51% of regulated entities had tested their incident response plans in the preceding 12 months, indicating an implementation gap consistent with the MAS score. These findings are supported by Hasan et al., (2023), who found that GCC Islamic banks exhibit stronger financial cybersecurity (Mal) but lag significantly in personal data governance (*Nasl*) and AI ethics (*aql*). Saudi Arabia's score therefore, does not reflect weak governance overall but a specific configuration of strong financial protection with underdeveloped data privacy and AI governance, a pattern that SAMA's 2024–2026 regulatory roadmap is beginning to address.

The UAE's CBUAE Circular 28/2023 requires enhanced digital onboarding due diligence; ADIB reported cybersecurity expenditure of AED 380 million (USD 103 million) in 2023, 2.1% of operating expenses, above the global financial services average of 1.7% (Gartner, 2023). The UK's strong MAS of 4.0, despite being a non-Muslim majority jurisdiction, demonstrates that robust secular frameworks can achieve high Maqasid alignment when the substantive protections addressed data privacy (UK GDPR → *hifz al nasl*), operational continuity (PRA operational resilience → *hifz al nafs*), and financial security (FCA SYSC → *hifz al mal*) overlap with *Maqasid* dimensions. This finding extends

Dusuki and Abdullah's (2007) argument that Maqasid compliance can be achieved through diverse institutional arrangements to the cybersecurity governance domain.

4.2 Cybersecurity Incidents Affecting Islamic Financial Institutions

Table 3 has been revised to include only cybersecurity incidents from within the five study jurisdictions, removing Bangladesh, which was not part of the research sample from the previous version. All incidents are sourced from official regulatory disclosures to ensure verifiability.

Table 3. Significant Cybersecurity Incidents Affecting Islamic and Global Financial Institutions (2019–2024)

Year	Jurisdiction	Incident Type	Scale / Loss	Maqasid Impact & Governance Implication
2021	United Arab Emirates (UAE) (Islamic banking sector)	Ransomware Attack on Islamic Banking Infrastructure	72-hour operational outage across multiple IFIs	*Hifz al Nafs*: service unavailability during Ramadan caused severe hardship during the sacred period; hifz al mal: customer funds temporarily inaccessible
2022	Saudi Arabia (sector wide IFIs)	Advanced Persistent Threat (APT) campaigns against SAMA regulated Islamic banks	14 major IFI intrusions reported (SAMA 2023)	*Hifz al Din*: risk of Shariah compliance monitoring system compromise; hifz al aql: intellectual property and strategic data theft from Islamic institutions
2022	United Kingdom (Al Rayan Bank)	Data Protection Breach customer PII exposure	ICO regulatory investigation initiated	*Hifz al Nasl*: personal PII data exposure violating customer dignity (karamah); *hifz al aql*: accuracy of customer records compromised
2023	Indonesia (Bank Syariah Indonesia BSI)	LockBit 3.0 Ransomware Attack	~15 million customer records exfiltrated; 5 day ATM and mobile banking outage	Multi Maqasid: *hifz al mal* (fund inaccessibility during Eid al Fitr), *hifz al nafs* (customer hardship during sacred period), *hifz al aql* (15 million records compromised)
2023	Malaysia (banking sector)	Mass Phishing and Social Engineering Campaigns	RM 2.4 billion losses across banking sector (BNM, 2023)	*Hifz al nasl* and *hifz al aql*: mass customer PII harvested; identity fraud targeting Islamic banking customers disproportionately
2024	United Arab Emirates (UAE) (sector wide)	AI powered Deepfake Fraud targeting Islamic banking customers	USD 25 million stolen from banking customers (CBUAE, 2024)	*Hifz al aql*: AI generated identity deception undermines rational decision making (*aql*); *hifz al mal*: direct financial theft from Islamic banking customers
2024	Indonesia (Bank Syariah Indonesia BSI)	Repeated Application System Disruptions	Multiple service outages totalling 6+ hours (OJK, 2024)	*Hifz al mal* and *hifz al nafs*: continued fund access disruption; demonstrates inadequate BCP implementation and failure to

Year	Jurisdiction	Incident Type	Scale / Loss	Maqasid Impact & Governance Implication
				remediate 2023 governance gaps

Source(s): IBM X Force (2023), IMF (2024), Interpol Financial Cybercrime Report (2023), OJK (2023), BNM (2024); Authors' compilation

The 2023 BSI incident directly validates three specific cells of the *maqasid* cybersecurity mapping matrix in Table 1. First, the *hifz al mal* cell's end-to-end encryption, MFA, and secure payment rails were breached by the LockBit encryption attack, confirming that ransomware exploits precisely the financial protection control gaps captured by the matrix. Second, the hifz al nafs cell's system availability (≥99.9% SLA) was violated by the five-day service outage during *Eid al Fitr*, validating the sacred period service continuity obligation identified in the framework. Third, the *hifz al aql* cell's 'data integrity' was compromised through exfiltration of 15 million customer records, confirming the governance gap reflected in Indonesia's MAS of 3.1. The multi-Maqasid nature of the BSI incident demonstrates a key characteristic of cybersecurity failures in Islamic banking contexts: a single incident can simultaneously violate multiple Maqasid dimensions, producing compounded harm disproportionate to the technical scope of the attack. This finding is consistent with Alam et al., (2023), who documented that jurisdictions with lower cybersecurity maturity scores experience significantly longer incident response times and larger breach scopes. Comparing across jurisdictions: the UK Al Rayan Bank breach (2022) primarily affected *hifz al nasl* through PII exposure, reflecting the UK's data privacy governance gap relative to its strong financial security controls. The UAE AI deepfake incident (2024) uniquely affected hifz al aql through AI-enabled identity deception, a new attack vector not captured by any existing cybersecurity governance framework, underscoring the need for the Maqasid AI ethics governance mapping proposed in Table 1 (Damayanti et al., 2024; Masrukhan et al., 2024).

4.3 Cross-Jurisdictional Cybersecurity Maturity and Maqasid Alignment

Table 4 presents granular maturity indicators, and Figure 1 visualises the MAS across jurisdictions, facilitating cross-jurisdictional comparison.

Table 4. Cross Jurisdictional Cybersecurity Maturity Indicators for Islamic Banks (2024)

Indicator	Malaysia	UAE	Saudi Arabia	Indonesia	United Kingdom
Dedicated Cyber Law (IFI specific)	Yes (PDPA+RMiT)	Yes (PDPL 2021)	Partial (ECC)	Partial (POJK)	Yes (UK GDPR+FCA)
IFSB GN 6 Compliance Level	Full	Full	Partial	Emerging	Full
IFIs with Incident Response Plan (%)	92%	88%	74%	61%	95%
Mandatory Data Encryption Policy	Yes	Yes	Partial	Partial	Yes
Third Party / Cloud Risk Policy	Mandatory	Mandatory	Advisory	Advisory	Mandatory

Indicator	Malaysia	UAE	Saudi Arabia	Indonesia	United Kingdom
Cybersecurity Audit Frequency	Annual	Annual	Biennial	Ad hoc	Annual
AI Ethics Guideline Published	Yes (2023)	Yes (2023)	Draft (2024)	Draft (2024)	Yes (2023)
SSB in Cyber Governance	Emerging	Emerging	Minimal	Minimal	Emerging
Avg. Breach Detection Time (days)	28	31	45	62	22
Cyber Budget (% Operating Exp.)	1.9%	2.1%	1.4%	0.8%	2.3%
Maqasid Alignment Score (MAS)	4.4	4.2	3.5	3.1	4.0

Source(s): IFSB (2024), BNM (2024), CBUAE (2023), SAMA (2023), OJK (2023), FCA (2024); Authors' compilation and scoring

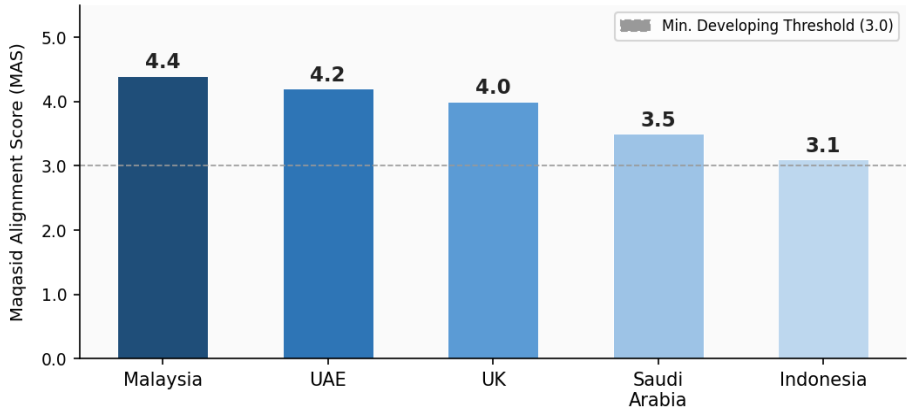

Figure 1. Maqasid Alignment Score (MAS) by Jurisdiction (2024)
Source(s): Authors' own work

The MAS score differences across jurisdictions are analytically significant, not marginal. The gap between Malaysia (4.4) and Indonesia (3.1) represents 26% of the maximum possible score, driven by a specific configuration of governance differences identifiable in Table 4: breach detection time (28 vs 62 days), cyber budget allocation (1.9% vs 0.8% of operating expenses), and cybersecurity audit frequency (annual vs ad hoc). This configurational pattern is consistent with QCA logic: governance outcomes are determined by combinations of conditions rather than single variables. The data are consistent with a directional relationship between regulatory density and Maqasid alignment, though the study makes no causal claim, as the QCA design cannot establish causality from N = 5 cases. This interpretive boundary is consistent with governance index methodology (Kaufmann et al., 2010). Critically, SSB involvement in cybersecurity governance is rated 'Emerging' at best across all five jurisdictions, confirming the universal governance gap identified as the study's primary finding.

The MAS benchmarks are consistent with findings from prior Islamic banking governance studies: Lassoued (2022) found that regulatory comprehensiveness is the primary predictor of cybersecurity governance quality in MENA Islamic banks, consistent

with Malaysia's leading MAS. Zahroh et al., (2024) documented Indonesian Islamic banking data governance maturity below regional peers, consistent with the MAS of 3.1. Arif et al., (2024) found 34% lower regulatory sanctions for data-compliant Malaysian IFIs, consistent with Malaysia's strong data protection scores in Table 4. The MAS framework, therefore, extends rather than contradicts prior empirical findings, providing a structured multidimensional instrument for governance comparison that supplements the individual variable analyses of prior studies. (Fadli et al., 2024; Mutmainah et al., 2024).

5. Conclusion And Recommendation

This study examined the impact of cybersecurity governance frameworks on the *Maqasid Al Shariah* alignment of Islamic Financial Institutions across five jurisdictions during 2019–2024. Using qualitative comparative analysis, the findings reveal that all five Maqasid objectives map systematically onto contemporary cybersecurity domains. The Maqasid Alignment Score (MAS) ranges from 3.1 (Indonesia) to 4.4 (Malaysia), indicating that regulatory maturity, Shariah specificity of frameworks, and enforcement mechanisms account for the majority of IFI cybersecurity governance variation across jurisdictions, consistent with bank intermediation theory (Diamond, 1984b) and Islamic finance governance scholarship (Iqbal & Mirakhor, 2011).

This study makes three principal theoretical contributions. First, it constructs the first systematic Maqasid cybersecurity mapping matrix applicable to global IFIs, extending *Maqasid Al Shariah* scholarship from financial product evaluation to digital governance, a domain not addressed in prior literature. The matrix operationalises all six Maqasid dimensions as evaluable governance criteria, providing a framework that future researchers can apply to additional jurisdictions, time periods, or institutional types. Second, the study incorporates *hifz al bi'ah* as a sixth *Maqasid* dimension in governance evaluation, contributing to contemporary *Maqasid* scholarship and operationalising Kamali (2025) theoretical extension in an empirical governance context for the first time. Third, the MAS provides a replicable, multidimensional governance benchmarking instrument that complements established secular governance indices by adding an Islamic ethical overlay. Future researchers can operationalise the MAS quantitatively by converting each scoring criterion into verifiable regulatory indicators, enabling cross-sectional regression analysis across larger samples, addressing the study's primary limitation and extending its empirical generalisability.

For Islamic Financial Institutions, the MAS functions as a practical self-assessment instrument: institutions can score themselves across the five governance dimensions by reviewing their own regulatory compliance, incident response capability, data encryption standards, SSB engagement, and AI governance documentation, then identify the specific dimensions where investment would yield the greatest governance improvement. For BSI specifically, the most immediately impactful reform is reducing breach detection time from the current 62-day average toward the 22-day UK benchmark, achievable through investment in automated threat detection and security information and event management (SIEM) systems, directly addressing hifz al mal obligations and potentially preventing a recurrence of the Eid al Fitr service disruption. Implementation challenges are significant:

smaller IFIs face resource constraints that make simultaneous compliance across all MAS dimensions financially prohibitive, suggesting a phased implementation approach prioritising hifz al mal controls (most directly tied to customer financial protection) before progressing to hifz al aql (AI ethics) and hifz al bi'ah (sustainability) requirements. For regulators Bank Indonesia, OJK, BNM, and SAMA, the highest impact reform requires only a regulatory directive rather than legislative change: mandating annual SSB review of technology risk governance, specifying at a minimum three agenda items: encryption standards review, incident response plan testing, and AI system bias audits. For Shariah Supervisory Boards, this study recommends formally incorporating technology risk into the annual Shariah audit agenda as an immediate action. Regarding the 'Shariah GDPR' recommendation: this proposal is grounded in the empirical finding that no jurisdiction in the study sample has a Shariah-specific data governance standard, creating a regulatory gap between secular GDPR type protections and the Islamic normative requirements of hifz al nasl. The proposal is feasible within the existing institutional structures of the IFSB and OIC Fiqh Academy, which have precedent for developing binding standards across jurisdictions. Similar cross-border standard setting has been successfully achieved through the IFSB's capital adequacy and liquidity standards, suggesting institutional readiness for a cybersecurity data governance equivalent.

At the societal level, stronger cybersecurity governance in Islamic banking directly supports the financial well-being, social stability, and religious trust of the global ummah. The BSI 2023 Eid al Fitr incident illustrates concretely how cybersecurity failures cause material and spiritual harm to Muslim communities: the five-day service disruption prevented millions of customers from making zakat payments, transferring remittances to family members, and accessing funds for Eid celebrations, affecting not only individuals' financial positions but also religious obligations and family relationships. These harms are disproportionately borne by financially vulnerable populations who rely most heavily on Islamic banking as their primary financial service provider. Improving cybersecurity governance, therefore, has direct distributional justice implications: it protects the most vulnerable segments of the ummah rural populations, small traders, and low-income earners from experiencing the severest consequences of IFI cyber incidents. At a societal level, sustained cybersecurity failures in Islamic banking risk eroding public confidence in Islamic financial institutions as trustworthy custodians of the ummah's wealth, potentially reversing decades of progress in Islamic banking market penetration and financial inclusion.

This study has four primary limitations. First, the MAS scoring relies on documentary evidence from regulatory publications, which may not fully capture implementation quality. A jurisdiction may have comprehensive regulations but poor enforcement; the MAS captures the former more reliably than the latter, and users of the MAS should interpret scores as 'de jure governance quality' rather than 'de facto operational effectiveness.' Second, the study analyses five jurisdictions representing 78% of global Islamic banking assets but excludes significant markets such as Pakistan, Turkey, Bangladesh, and Sub-Saharan Africa; findings should not be generalised to those markets without further empirical validation. Third, equal weighting of MAS dimensions may not reflect the relative jurisprudential priority of Maqasid dimensions; future research should develop expert-weighted MAS variants using Delphi methodology to capture Shariah scholars' prioritisation preferences. Fourth, scoring reflects

a single period (2019–2024) and may not capture regulatory changes occurring after data collection. Future research should: (1) extend the MAS framework quantitatively across 20+ jurisdictions to identify causal determinants of Maqasid alignment; (2) apply the framework to Islamic microfinance institutions and Islamic FinTech platforms, which face distinct cybersecurity challenges; (3) conduct longitudinal MAS tracking to measure governance improvement trajectories post regulatory reform; and (4) explore hifz al bi'ah empirically through Islamic banks' sustainability and environmental data governance reporting (Permana & Ikasari, 2023).

Declaration

Authorship

All authors actively participated in the work and have agreed to the final version of the manuscript

Author Contribution Statement

Bintang Junita (First Author) led the overall research conceptualization, developed the Maqasid cybersecurity mapping matrix, conducted the Qualitative Comparative Analysis (QCA), and drafted the core sections of the manuscript. Dicky Octaviano (Corresponding Author) contributed to framework refinement, data analysis, policy recommendations, and final manuscript editing. Zulfati Dinul Fatiha contributed to the literature review, regulatory data collection across jurisdictions, and revision of the theoretical mapping. Muhammad Senoyodha Brennaf provided comparative insights on the United Kingdom jurisdiction, assisted with cybersecurity incident analysis, and reviewed the discussion and recommendations.

Funding Statement

This research received no specific grant from any funding agency in the public, commercial, or not-for-profit sectors.

Data Availability Statement

This research relies on secondary data from publicly available regulatory publications (2019 2024), IFI annual reports, IFSB standards, and global cybersecurity databases. All data sources are cited in the manuscript and are openly accessible.

Declaration of Interests Statement

The authors declare that there are no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

References

Al-Ghazali, A. H. M. (1993). *Ihya Ulum al-Din*. Dar al-Khayr.

Alharbi, A., Sbeiti, W., & Ahmad, M. (2024). Money supply, banking and economic growth: A cross-country analysis. *International Journal of Economics and Financial Issues*, *14*(2), 234–242. https://doi.org/10.32479/ijefi.15749

Al-Nawawi, Y. (1900). *Al-Arba'in al-Nawawiyyah*.

Al-Shatibi, I. (2004). *Al-Muwafaqat fi Usul al-Shariah* (Vols. 1–4). Dar al-Ma'rifa.

Anisak, & Bakhri, S. (2024). Meningkatkan inklusi keungan melalui produk mikro syariah. *REVENUE: Jurnal Ekonomi Pembangunan Dan Ekonomi Islam*, *7*(2).

Chapra, M. U. (2008). *The Islamic vision of development in the light of Maqasid al-Shariah*.

Damayanti, D., Nasution, M., & Sudiarti, S. (2024). Analisis harga pokok produksi dengan metode full costing sebagai alat bantu perencanaan laba (Studi kasus Ayam Penyet Sahabat Solo) [Analysis

of cost of goods manufactured using the full costing method as a profit planning tool (Case study: Ayam Penyet Sahabat Solo)]. *Jurnal Ilmiah Manajemen, Ekonomi, & Akuntansi (MEA)*, *8*(2), 1127–1141.

Diamond, D. W. (1984a). Financial intermediation and delegated monitoring. *Review of Economics Studies*, 393–414.

Diamond, D. W. (1984b). Financial intermediation and delegated monitoring. *Review of Economic Studies*, 393–414.

Dusuki, A. W., & Abdullah, N. I. (2007). Maqasid al-Shariah, Maslahah, and corporate social responsibility. *The American Journal of Islamic Social Sciences*, *24*(1), 25–45.

Fadli, A., Widayatsari, A., & Setiawan, D. (2024). Analisis jalur pengaruh bi-rate dan jumlah uang beredar terhadap pertumbuhan ekonomi di Indonesia. *E-Mabis*, *25*(1), 47–54. https://doi.org/10.29103/e-mabis.v25i1.1271

Fasa, I. (2020). *Eksistensi Bisnis Islami Di Era Revolusi Industri 4.0*. Widina Bhakti Persada.

Fatoni, A., & Sidiq, S. (2019). Analisis perbandingan stabilitas sistem perbankan Syariah dan Konvensional di Indonesia. *Ekspansi: Jurnal Ekonomi, Keuangan, Perbankan Dan Akuntansi*, *11*(2), 179–198. https://doi.org/https://doi.org/10.35313/ekspansi.v11i2.1350

Freeman, R. E. (1984). *Strategic Management: A Stakeholder Approach*. Pitman Publishing.

Gartner. (2023). *IT Key Metrics Data 2023: Financial Services Industry Security Spending*.

Grassa, R., & Matoussi, H. (2014). Corporate governance of Islamic banks: A comparative study between GCC and Southeast Asia countries. *International Journal of Islamic and Middle Eastern Finance and Management*, *7*(3), 346–362.

Hasan, Z., & Asutay, M. (2011a). An analysis of the courts' decisions on Islamic finance disputes. *ISRA International Journal of Islamic Finance*, *3*(2), 41–71.

Hasan, Z., & Asutay, M. (2011b). An analysis of the courts' decisions on Islamic finance disputes. *ISRA International Journal of Islamic Finance*, *3*(2), 41–71.

Hassan, M. K., & Lewis, M. K. (2007). *Handbook of Islamic banking*. Edward Elgar Publishing.

Interpol. (2023). *Financial Cybercrime Report 2023*. Interpol General Secretariat.

Iqbal, Z., & Mirakhor, A. (2011). *An introduction to Islamic finance: Theory and practice*. Wiley.

Kamali, M. H. (2012). *Maqasid al-Shariah, Ijtihad and civilisational renewal*. International Institute of Advanced Islamic Studies.

Malfiandri, Zulkan, & Radimin. (2025). Menakar stabilitas sistem keuangan nasional: Analisis dampak dual banking system di Indonesia. *Jurnal Akuntansi, Keuangan, Perpajakan Dan Tata Kelola Perusahaan (JAKPT)*, *2*(4), 1141–1150.

Mamuaja, R. C., Saerang, I. S., & Tasik, H. H. D. (2024). Analisis pengaruh uang beredar, suku bunga, dan inflasi terhadap pertumbuhan kredit perbankan di Indonesia sebelum dan sesudah pandemi Covid-19. *Jurnal EMBA*, *12*(3), 892–901.

Mankiw, N. G. (2019). *Macroeconomics*. Worth Publishers.

Masrukhan, M., Rahmah, N., Sella, W. N., & Jannah, L. (2024). Literature review: Dampak merger Bank Syariah Indonesia (BSI) terhadap karyawan dan nasabah. *Jurnal Nuansa: Publikasi Ilmu Manajemen Dan Ekonomi Syariah*, *2*(4).

Mishkin, F. S., & Eakins, S. G. (2021). *Financial Markets and Institutions: 9th ed.* Pearson.

Mutmainah, A., Khairiyah, D. C., Nasution, H. R., Sambo, R. A., & Cahya, S. D. (2024). Kajian peran kebijakan moneter syariah dalam mendorong pertumbuhan ekonomi Indonesia. *Indonesian Research Journal on Education*, *4*(2), 567–573. https://doi.org/https://doi.org/10.31004/irje.v4i2.613

Nouman, M., Hashim, M., Trifan, V. A., Spinu, A. E., Siddiqi, M. F., & Khan, F. U. (2022). Interest rate volatility and financing of Islamic banks. *PLoS ONE*, *17*(7). https://doi.org/https://doi.org/10.1371/journal.pone.0268906

Pamungkas, P., Septianto, F., & Trinugroho, I. (2025). Monetary policy via bank lending channel: Evidence from lending decomposition. *Journal of Risk and Financial Management*, *18*(5). https://doi.org/10.3390/jrfm18050249

Permana, R. A., & Ikasari, D. (2023). Uji normalitas data menggunakan metode empirical distribution function dengan memanfaatkan MATLAB dan MINITAB 19. *Seminar Nasional Riset Dan Inovasi Teknologi*, 7–12.

Qibtiyah, M., & Wicaksono, F. (2022). Analisis merger bank syari'ah Indonesia (BSI) dalam perkembangan perbankan syari'ah di Indonesia. *Jurnal*, *6*(2), 581–595.

Rahmatika, A. N., & Romadhani, N. P. (2021). Dual banking system paska merger di Indonesia. *Dinamika*, *6*(1), 77–90.

Siregar, F. D., Lubis, A. S., & Daulay, A. (2025). *Peran bank syariah dalam stabilitas moneter: Pendekatan ekonomi Islam*. *17*(1), 140–144.

World Bank. (2023). *Indonesia Economic Prospects: Making the Most of the Next Stage of Growth*.

This page is intentionally left blank
(*this sheet is for odd-numbered end pages of articles*)