IFSB WORKING PAPER SERIES
WP-27/12/2023

REGULATORY PRACTICES IN DIGITAL ISLAMIC BANKING

DECEMBER 2023

ISLAMIC FINANCIAL SERVICES BOARD

IFSB WORKING PAPER SERIES
Standards Development and Research Department

WP-27/12/2023

REGULATORY PRACTICES IN DIGITAL ISLAMIC BANKING

Abideen Adewale
Kazi Md. Masum

December 2023

Corresponding email: research@ifsb.org

This working paper has benefited from the feedback and guidance provided by the Acting Assistant Secretary-General, Aminath Amany Ahmed and the members of the Standards Development and Research Department of the IFSB and members of the IFSB Technical Committee who reviewed the draft paper. The authors are grateful to all IFSB members who participated in the survey, and for providing useful comments on the draft paper during members' consultation.

Published by: Islamic Financial Services Board

Level 5, Sasana Kijang, Bank Negara Malaysia

2, Jalan Dato' Onn, 50480 Kuala Lumpur, Malaysia

Email: ifsb_sec@ifsb.org; research@ifsb.org

ABOUT THE ISLAMIC FINANCIAL SERVICES BOARD (IFSB)

The IFSB is an international standard-setting organisation which was officially inaugurated on 3 November 2002 and started operations on 10 March 2003. The organisation promotes and enhances the soundness and stability of the Islamic financial services industry by issuing global prudential standards and guiding principles for the industry, broadly defined to include banking, capital markets and insurance sectors. The standards prepared by the IFSB follow a lengthy due process as outlined in its Guidelines and Procedures for the Preparation of Standards/Guidelines, which includes issuing exposure drafts and holding workshops and, where necessary, public hearings. The IFSB also conducts research and coordinates initiatives on industry-related issues, and organises roundtables, seminars and conferences for regulators and industry stakeholders. Towards this end, the IFSB works closely with relevant international, regional and national organisations, research/educational institutions and market players.

For more information about the IFSB, please visit **www.ifsb.org**.

ABSTRACT

Digital banking has revolutionised the financial landscape, presenting novel services, enhanced convenience, and expanded access to financial offerings. Nevertheless, these advantages come with distinctive risks and challenges that necessitate robust regulatory frameworks to preserve financial stability and safeguard consumers. This paper delves into the regulatory environment encompassing digital banking, emphasising the pivotal role of regulatory authorities in ensuring efficient risk management, capital sufficiency, and adherence to pertinent legislation.

The research explores the cautious approach embraced by regulatory and supervisory authorities (RSAs) in striking a balance between fostering financial innovation and competition while safeguarding market integrity and consumer interests. It investigates how some jurisdictions have adopted tailored regulations for digital Islamic banking, while others have adapted existing frameworks for their application. Furthermore, the study discusses the potential hurdles faced by RSAs in effectively overseeing digital Islamic banks, especially concerning data privacy, cybersecurity, and compliance with Anti-Money Laundering (AML) and Combating the Financing of Terrorism (CFT) regulations. There are concerns about the need for Sharī‘ah considerations in digital products and financial applications development in response to the perceived “Sharī‘ah neutrality” of technology.

As the popularity of digital Islamic banking continues to grow, the need for comprehensive regulatory frameworks becomes increasingly evident. The research predicts a rise in regulatory adoption in jurisdictions currently lacking specific frameworks, driven by RSAs' cumulative experience in managing these emerging financial institutions. Additionally, the study underscores the importance of prioritising customer protection and promoting financial inclusion in resolution plans for digital banks.

TABLE OF CONTENTS

ABBREVIATIONS

AML	Anti-Money Laundering
CFT	Combating the Financing of Terrorism
CGAP	Consultive Group to Assist the Poor
E-KYC	Electronic-Know Your Customer
FATF	Financial Action Task Force
FSDP	Financial Sector Development Program
HQLA	High-Quality Liquid Assets
IFSB	Islamic Financial Services Board
IFSI	Islamic Financial Services Industry
KYC	Know Your Customer
LCR	Liquid Coverage Ratio
ML/FT	Money Laundering/Financing of Terrorism
MSME	Micro, Small, And Medium Enterprises
NSFR	Net Stable Funding Ratio
OIC	Organisation of Islamic Cooperation
PSPR	Payment Services Provider Regulations
RSA	Regulatory And Supervisory Authorities
SNCR	Sharīʿah Non-Compliance Risk
SVF	Stored Value Facilities
TN	Technical Note
UAE	The United Arab Emirates

Section 1: Introduction

1.1. Background

Technological advances present new regulatory and supervisory opportunities and challenges for financial sector regulators. The topic of digital banking regulation continues to gain traction among policymakers and regulatory and supervisory authorities (RSAs) across many jurisdictions. Generally, regulation sets the rules and exerts influence on innovation, but sometimes the reverse is true.[1] Rapid technological advancements, changing competitors and competition, and centricity on customer structural dynamics and preferences continue to transform the business model, products, and services of financial institutions. Some aspects of regulatory and supervisory frameworks may be based on activities and risks rather than solely on the entity undertaking them. These not only raise new operational concerns but also supervisory and regulatory questions, especially in jurisdictions with limited requisite capacity and resources.

Due to the specificities of Islamic banking and the constantly changing nature of technology, the regulation and supervision of digital Islamic banking also continues to evolve and vary across jurisdictions. This depends on a number of factors including but not limited to regulatory culture,[2] policy objectives, market maturity, and availability of both financial and non-financial enablers, etc. Generally, RSAs have been cautious about coordinating prudential regulation, financial innovation, and competition policy. They have had to find a balance between ensuring that a favourable disposition towards technological financial innovation does not infringe on financial market integrity and stability and protecting consumers.

RSAs in jurisdictions where Islamic banking is practiced are adopting different regulatory approaches towards the digitalisation of banking operations to support broader policy objectives like financial inclusion, contestability, competition, customer value,[3] etc. For instance, some jurisdictions have responded by developing bespoke regulations for digital Islamic banking, while others have adapted and applied extant banking regulations to digital banks, including those based on Islamic principles. And despite digital banking's inevitability as the financial market evolves, some other jurisdictions do not yet have any related regulatory framework in place.

RSAs encounter various challenges that can impede their regulatory and supervisory oversight of digital Islamic banks. One such challenge is the lack of technological expertise, which hampers their understanding and evaluation of innovative business models and practices presented by the blend of technological innovations and specificities of Islamic banking practice. This can also impede adequate understanding during the Sharī'ah review and product approval process. For example, the Sharī'ah committee at the digital Islamic banking level and, where it exists, the Sharī'ah council at the supervisory level, bears significant responsibility for overseeing and addressing any instances of Sharī'ah non-

[1] While regulation reacts to market dynamics, it also proactively opens up the competitive space in the financial sector. For instance, in August 2020, the Saudi Central Bank (SAMA) revised the Payment Services Provider Regulations (PSPR) to align with the European Union's Payment Services Directive (PSD2). This update requires banks to allow authorized third-party entities access to customer bank accounts for payment initiation and account information services.

[2] While some countries prioritise innovation to enhance customer outcomes, others prioritise standardised requirements that can be regulated in the interest of the customers.

[3] Abideen A. IFSB Working Paper 19 (2020).

compliance that may arise from innovative financial products and processes within digital Islamic banking institutions. This oversight should also extend to aspects of product design, including Islamic banking apps, to ensure adherence to Sharīʿah principles throughout the contractual relationship, as well as in relation to rights of contracting parties, beneficial ownership, and other relevant areas in accordance with Islamic jurisprudence.

Additionally, Islamic banking innovations may not fit traditional definitions of financial services, posing challenges for direct regulatory oversight that relies on prudential requirements. Therefore, reviewing regulatory and supervisory frameworks for digital Islamic banking requires a focus on the specific activities and risks involved, rather than solely on the entities undertaking them. Regulations thus need to play a vital role in ensuring that institutions effectively manage risks, especially those peculiar to the business model of the digital Islamic banks, for example, to ensure adequate capital and liquidity maintenance or resolution of institutional failures without disrupting the overall system or burdening the public with costs.

Regulators also face resource constraints, especially in the context of technology-driven advancements that rely heavily on data and may involve multiple regulatory bodies and external third parties. Cloud computing, for instance, has gained significant traction in the banking industry, particularly for unbundling services and data sharing in open banking applications. According to an IFSB survey, 57% of Islamic banks have adopted cloud technology, indicating a shift from on-premises data services to public cloud-based data services. This adoption offers the potential for cost reduction in infrastructure and human resources, as Islamic banks can outsource technology through various vendors and platforms providing cloud services. However, certain considerations must be addressed, as these Islamic banks may need to provide financial services on platforms they do not own or directly control. This poses potential implications for financial stability in the event of a breach or cyber-attack targeting the cloud service provider, particularly since these activities fall outside the regulatory oversight of RSAs.

With the inevitable growth of digital Islamic banking and with more licensed digital Islamic banks becoming operational, further regulatory developments will be seen across jurisdictions as RSAs accumulate invaluable experience. Such regulatory change is also envisioned to be more common both in jurisdictions with no regulations currently, and those that have adopted or adapted existing regulatory and supervisory frameworks in favour of bespoke regulations for their digital Islamic banking institutions.

This working paper aims to understand the regulatory and supervisory landscape via discussion and comparison of the various regulatory and supervisory regimes and approaches for digital Islamic banking. The specific aim is to highlight commonalities and distinctions across jurisdictions where it is practised.

The remainder of this working paper is organised as follows. This section also presents a brief description of the survey methodology and information about the respondent IFSB RSA Members. Section 2 focuses on the regulation of Islamic digital banking and specifically covers issues relating to regulatory regimes, regulatory drivers, and the review process. Section 3 focuses on the supervisory aspects of Islamic digital banking and specifically covers issues relating to prudential considerations, supervisory obstacles, and supervisory innovations.

Section 4 provides the conclusion based on the findings and recommendations for further actions.

1.2 Survey Methodology

In addition to conducting an extensive desk review of extant related regulations and other official documents from various jurisdictions, the information provided in this paper is based on the data collected via a questionnaire survey administered to the IFSB RSA Members. The survey comprised mainly closed-ended questions with codes to indicate options a respondent RSA might wish to select. In some other instances, open-ended questions were also included for the respondent RSAs to freely express an opinion on related matters beyond the closed-ended options provided. The cooperation of the responding RSAs was sought to ensure that the responding officer was the person with the relevant responsibility to do so, and that the permission of relevant superiors or authorities was obtained where necessary. The responses provided by an institution are assumed to reflect its perspectives on the issues raised. Owing to the exploratory nature of the research, data were elicited from 13 IFSB member organisations;[4] eight are from systemically significant jurisdictions.[5] Data obtained were subjected to descriptive data analysis only, mainly based on simple percentage and frequency analysis. Furthermore, in addition to insights provided by experts during the inaugural IFSB Consultative Group (ICG) meeting and IFSB RSA members' consultation, focused interviews were also conducted with two more RSAs to gain more insights into the regulatory and supervisory practices of digital Islamic banks.

[4] The list is provided in Appendix A.

[5] The share of Islamic banking assets is at least 15 percent of total value of domestic banking assets.

Section 2: Analyses and Discussion of Survey Responses

2.1 Terms and Definition of Digital Islamic Banking

The survey responses indicate that the concept and definition of digital Islamic banking vary across jurisdictions, perhaps due to its early stages of development and the different approaches taken by various jurisdictions. In certain jurisdictions, the emphasis is on the platforms used to deliver these services, which distinguishes them from traditional Islamic banking. On the other hand, in some cases, digital Islamic banking is seen as a means of providing traditional banking services while utilising technology to enhance efficiency, data security, regulatory compliance, and the overall customer experience.

In the jurisdictions that conceptualise Islamic digital banking based on the channel of delivery, some allow a limited physical presence[6] beyond their main place of business, while the core banking activities are carried out first or mainly through digital channels. For instance, in Malaysia Islamic digital banking business is defined as Islamic banking business[7] that is carried on wholly or almost wholly through digital or electronic means. Similarly, the Saudi Central Bank (SAMA) retained extant regulations but provided more clarity as per the additional guidelines for digital-only banks issued in February 2020 where it defines a digital bank as one that conducts banking business mainly through digital channels.

In some other jurisdictions, the digital operations of institutions offering Islamic financial services are regulated based on the permissions granted by their operating license. For example, in Pakistan, the *Licensing and Regulatory Framework for Digital Banks* recognizes digital banking activities as various services conducted through digital channels such as the internet, mobile applications, automated teller machines, and point-of-sale services. These services can be offered by either conventional or Islamic banks. On the other hand, in Bahrain, although there is no specific definition for “Digital Banking”, regulated services provided through digital channels generally fall within the scope of digital banking activities, including services like “digital financial advice”, “open banking”, and “digital onboarding”. Islamic bank licensees in Bahrain have the option to open customer accounts through a digital onboarding process facilitated by the National Electronic-Know Your Customer (E-KYC) system.

Digital Islamic banking is also perceived as a means of providing traditional banking services while leveraging technology to improve operations. For instance, in some jurisdictions like Maldives and Sudan, digital Islamic banks may not exist in a strict sense of being identified as such. However, Islamic banks and Islamic banking windows in these jurisdictions offer services such as online banking, mobile banking, mobile wallets, etc. through digital platforms.

Some respondent RSAs indicated that in their jurisdiction, a digital Islamic bank, though not yet in existence, would be considered a pure-play digital financial institution. In this case, regulations bar Islamic banks from having physical points of business with customers. For example, in the Philippines, digital banks are a distinct category, defined as banks that offer financial products and services that are processed end-to-end through a

[6] This is to handle customer complaints, especially in special circumstances, for instance, fraud.
[7] Section 2(1) of the Islamic Financial Services Act 2013

digital platform and/or electronic channels with no physical branch/sub-branch or branch-like unit offering financial products and services. This, however, does not prohibit the current lone Islamic bank and other "prospect" Islamic banks in the country from offering products and services via digital platforms. As another example, the Bank of Mauritius issued a Guideline for Digital Banks in December 2021, which applies to a bank licensed to carry on exclusively private banking business or exclusively Islamic banking business solely through digital means or through electronic delivery channels under section 52(1) of the Banking Act 2004. The regulation completely bars digital banks from having physical points of business with customers.

While some jurisdictions have applied the same regulatory framework to entities offering digital Islamic banking services as they do to traditional banks, regulation and supervision considers their specific risk profile and any additional risks they may be subject to. For example, the Dubai Financial Services Authority (DFSA) applies the same regulatory framework to entities offering digital Islamic banking services as it does to any other bank operating within the Dubai International Financial Centre (DIFC). In this jurisdiction, there is no specific definition of "digital Islamic banking." Any entity providing banking services or conducting banking activities within or from the DIFC, whether digitally or not, is subject to the relevant laws, rules, and regulations. The regulation and supervision of such entities are determined based on their risks; a "digital bank" would be subject to additional risks associated with technology or the digital delivery of services. Similarly in Indonesia, although the Otoritas Jasa Keuangan (OJK) has amended the banking regulation, no special status is accorded either the conventional or Islamic digital banks despite their distinct business models and associated risk management and governance requirements.

The definition and classification of digital Islamic banking present a challenge across jurisdictions. The lack of clear differentiation between Islamic banking digital channels, digitised traditional Islamic banks, and fully digital Islamic banks raises questions about how digital Islamic banking is conceptualised. The varying interpretations and definitions of these categories have implications for supervision and regulation.

There is also a question of whether a traditional Islamic bank that decides to digitise a significant portion of its operations would require a new license. Indonesia provides an illustrative example where the OJK mandates that traditional banks meeting the criteria of a digital bank must undergo conversion to ensure regulatory compliance. Likewise, in the Philippines, the Bangko Sentral Ng Pilipinas (BSP) has established specific provisions for licensed financial institutions seeking to convert into digital banks. This conversion can be voluntary or mandatory, depending on whether the regulatory authority determines that the existing bank already meets the requirements to be classified as a digital bank. The conversion process involves the closure of all physical branches and the adjustment of services within a three-year timeframe.

Table 1. Terms and Definition of Islamic Digital Banks in Various Jurisdictions.

AUTHORITY	TERM	DEFINITION
Bank Negara Malaysia	Islamic Digital Banks	Carries out banking business wholly or almost wholly through digital or electronic means

Bangko Sentral Ng Pilipinas – Philippines	Digital Banks	Offers financial products and services through digital platforms and/or electronic channels with no physical branch[8]
State Bank of Pakistan	Digital Banks	Provides services predominately through digital and electronic means and has no physical branches[9]
Saudi Central Bank	Digital Banks	Conducts banking businesses mainly through digital channels
Bank of Mauritius	Digital Banks	Provides services solely through digital means or through electronic delivery channels; Islamic or conventional bank
Dubai Financial Service Authority	No definite term	Holds all banks to the same regulation regardless of whether their business model is digital or traditional.
Banking Regulation and Supervision Agency, Turkey	Digital Banks	Credit institution that provides banking services through electronic banking services distribution channels instead of physical branches.[10]
Central Bank of Bahrain	Digital Banks	Although no definite term exists, generally, regulated services provided through digital channels will fall under digital banking activities. For example, “digital financial advice”, “open banking”, and “digital onboarding”.
The Central Bank of Sudan	Islamic Digital Banks	Offers services such as mobile banking, mobile wallets, online banking, and online account opening
Maldives Monetary Authority	No definite term	Islamic banks and Islamic banking windows offering services via digital platforms

Source: IFSB Survey 2023.

2.2 Driving Factors for Regulation of Digital Islamic Banking Across Jurisdictions

Several reasons were identified as the driving forces behind the development of regulatory and supervisory frameworks for digital Islamic banking in respective jurisdictions. In general, the motivations comprise diverse factors, such as government policies, industry requirements, comparisons with other jurisdictions, risk management, promotion of stability, and ensuring the protection of consumers.

All survey respondents agree that government policies and strategies aimed at promoting socio-economic development play a significant role in driving the adoption and expansion of digital banking. These policies focus on key areas such as fostering financial inclusion, supporting micro, small, and medium enterprises (MSMEs), and empowering women and youth. By leveraging digital financial services, these policies aim to increase access and participation in the economy, promoting inclusive growth.

For example, Saudi Arabia’s digital banking framework was developed in consideration of the sector’s emergence and aligned with the objectives of the Kingdom’s Financial Sector Development Program (FSDP). Similarly, in Pakistan, the regulatory framework for digital banking is influenced by a combination of factors, including government policies for socioeconomic development, industry requests, and the growing prominence of the digital banking sector, as well as emerging supervisory evidence. Objectives such as promoting financial inclusion, providing credit access to underserved populations, offering affordable and

[8] Digital banks are required to maintain a principal/head office in the Philippines to serve as the main point of contact.
[9] State Bank of Pakistan (2021)
[10] Erdemir & Özmen Attorney Partnership (2021)

efficient digital financial services, fostering financial technology and innovation, improving customer experiences, and developing the digital ecosystem all contribute to shaping the regulatory approach for digital banking. In Malaysia and Pakistan, the Bank Negara Malaysia and State Bank of Pakistan, respectively, explicitly mentioned enhancing financial inclusion, financial well-being, and sustainable growth in line with the Sharī'ah while safeguarding financial system stability and customer protection in the licensing framework as a key consideration for operating digital Islamic banking.

Some respondents also indicated that the customer base of Islamic banks plays a role in promoting financial inclusion via digital Islamic banking. This becomes especially pertinent given the features of the demographic structure of Muslims as the primary patrons of Islamic banks. For instance, the median age among Muslims worldwide is 24, while 15 out of the top 59 countries with high smartphone penetration – the main instrument used for digital banking – are members of the Organisation of Islamic Conference (OIC), and where 72% of the global unbanked population resides. Despite notable digital Islamic banking-related efforts, financial inclusion remains highly uneven across countries within the Arab region, with significant percentages of male adults lacking access to accounts and MSMEs lacking access to finance. Consultive Group to Assist the Poor (CGAP) reports a large number of financially excluded adults and unfinanced companies in the Arab region, presenting a significant opportunity for digital Islamic banking to use technology and innovation to address these gaps, particularly in targeting specific groups such as youth, women, refugees, and low-income individuals.

Another prominent motivation for developing digital Islamic banking regulation is the analysis of how other jurisdictions regulate Islamic digital banking. Regulators can learn from successful regulatory frameworks and best practices in key regional and global developed markets and adapt them to their own circumstances, ensuring appropriate oversight and fostering growth within the sector. In Saudi Arabia for instance, the Saudi Central Bank (SAMA) amended its Payment Services Provider Regulations (PSPR) by incorporating principles implemented by the European Union's Payment Services Directive (PSD2) to allow more convenience for international Payment Service Providers (PSPs) operating in Saudi Arabia.

Industry stakeholders' demands and requests also significantly influence the motivation for regulating digital banking. As the digital banking sector continues to grow, some respondent RSAs indicate that industry players seek clear regulations and guidance to establish a favourable operating environment. Issues relating to regulatory uncertainty are among the least-cited impediments to the digital transformation process in Islamic banking as per the IFSB survey. Responding to these requests can create an enabling atmosphere for digital banking operations and encourage further innovation.

Moreover, the increasing prominence and size of the digital banking sector itself can serve as a motivation for regulation. Recognising the need to address associated risks, protect consumers, and promote stability, regulators are compelled to establish comprehensive regulatory frameworks that ensure the proper functioning and integrity of the digital banking industry.

RSAs were asked if they envisage any changes in the Islamic digital banking regulation in their jurisdiction in the near future, or when they expect such changes to take place. The majority of RSA respondents indicated that they do not have immediate plans to change the regulation of digital Islamic banking. However, among those anticipating changes, 50% expect them to occur within the next year, while the other 50% foresee changes taking place in 4-5 years. Saudi Arabia is among the countries expecting regulatory changes in the near future, as it considers establishing a legal framework to regulate financial technology within the banking sector. This comprehensive framework would include general provisions and specific regulations covering areas such as digital banking, open banking, regulatory technology (Regtech), and big data. Similarly, Bahrain is likely to focus on developing more customised regulatory frameworks for digital banks, suggesting a potential evolution in its regulatory approach.

2.3 Digital Islamic Banking Regulatory Regimes Across Jurisdictions

In most jurisdictions, central banks are primarily responsible for regulating digital Islamic banks. In jurisdictions that indicated they had adopted existing regulations, the response to the question on regulatory obligations expected of Islamic digital banks was that digital Islamic banks must diligently adhere to essential regulatory obligations. These include establishing a secure and trustworthy financial ecosystem that prioritises protecting customers, combatting financial crimes, ensuring prudential soundness and resilience, and promoting transparency and stability within the industry.

Responses also indicated that a crucial mandate for digital banks is to maintain accurate and comprehensive communications with customers. Transparent and truthful interactions serve as the primary touchpoint, empowering customers to make well-informed decisions. This includes providing in-depth information about products, services, fees, and potential risks, as well as offering standardised information with explicit risk warnings, cost disclosures, and transparent terms and conditions.

There are three discernible approaches to regulating digital Islamic banking across jurisdictions: phased licensing, bespoke, and common licensing regulatory regimes.

Phased Licensing Regulatory Regime

Some respondent jurisdictions adopt a phased authorisation regime wherein they rely on existing regulations for digital Islamic banks and grant new entrants a specific license with initial activity restrictions. This approach allows for more flexible regulatory requirements, reduced capital investments, and limitations on permitted activities before becoming a full-fledged digital Islamic bank. All respondent RSAs adopting existing regulations for their digital Islamic banking also indicated that they consider such regulations as being prescriptive enough in terms of permitted or restricted activities, prudential requirements, and expected obligations.

In jurisdictions where a phased approach is adopted, there is usually a stated period for new digital banks to fulfil all requirements for a full-fledged bank. The phased authorisation period therefore entails limited prudential requirements, for instance, on capital, liquidity, deposits etc, and also limited permitted activities. A notable example of a jurisdiction following this regime for its digital Islamic banking segment is Malaysia. Specifically, the

licensing framework[11] takes a balanced approach to allow the entry of digital banks with strong value propositions while ensuring the integrity, stability, and protection of depositors within the financial system. This approach allows licensed digital banks to grow their investments, attract more capital, strengthen their information technology architecture, build staff capacity, and streamline contracts with the numerous third parties archetypical of their banking business model. It also allows digital banks to perfect recovery and business continuity plans, and engage more closely with RSAs to attenuate any regulatory uncertainty.

To achieve these goals, digital banks initially operate under a simplified regulatory framework, specifically tailored to their operations, for a period of three to five years or until their assets reach a maximum threshold of RM 3 billion. To exit the foundational phase, a licensed Islamic digital bank would have to comply with the regulatory requirements applicable to an existing licensed Islamic bank. The framework also provides clarification on selected areas specific to digital banks, such as business activities and physical presence, in addition to the existing regulatory framework for banks, including capital adequacy, liquidity, stress testing, Sharī'ah governance, and public disclosure requirements. Digital banks, whether Islamic or conventional, are required to comply with the Islamic Financial Services Act 2013 or Financial Services Act 2013, as well as adhere to prudential standards, Sharī'ah principles, business conduct guidelines, consumer protection measures, and regulations concerning anti-money laundering and countering the financing of terrorism.

Nonetheless, there are arguments about whether such a phased regulatory regime should adopt a broad-brush approach or be applied within a range of classifications to accommodate the different peculiarities of digital banks. For instance, in a mandatory periodic phased authorisation period, the growth and scaling of a digital bank that already has all the prudential and operational requirements may be inadvertently limited. Conversely, the period may also be too short for some other digital banking applicants, which may result in eventual revocation of license and avoidable collateral reputational damage for a business model that remains nascent but is also quickly evolving. However, a case-by-case consideration of each of the digital banking applicants vis-à-vis their specific requirements would entail more human and financial resources from the RSAs.

Bespoke Regulatory Regime

Only a few jurisdictions adopt customised digital banking licenses with limitations on physical presence without altering traditional banking requirements. A notable driver for this, as in the case of Pakistan, is usually a national policy objective such as broadening financial inclusion and deepening the local Islamic banking industry via technological innovation. This regulatory regime for digital Islamic banks raises a question related to the limited physical presence or non-permission for opening branches. In jurisdictions where this is practiced, it raises a question of what the protocol would be if circumstances necessitate a physical point of business. Furthermore, most of the financially excluded population are likely to have no or little knowledge of relevant technology and to reside in rural areas where technological infrastructure may not be available.

[11] Bank Negara Malaysia, (2020)

Moreover, in many jurisdictions where Islamic banking is prominent, transactions are still very much cash based. This can be as much as 75% of transactions, even in countries with advanced infrastructures. In jurisdictions where technological infrastructure is poor and/or during a downtime or network failure, customers may not have alternative access to cash.

Bespoke digital banking licenses may attract new entrants, especially in jurisdictions where Islamic banking is still marginal. However, there are already numerous new entrant fintech firms offering various digital financial services that, in a bid to avoid regulation and compliance costs, would opt not to become licensed Islamic digital banks to perform other crucial services like taking deposits.

Common Digital Bank Licensing Regime

In some other jurisdictions, the respondent RSAs indicate that the same regulatory and supervisory regimes apply to all banks regardless of whether they are Islamic or conventional, digital or traditional. Such regimes are viewed as providing a level playing field to mitigate regulatory arbitrage and regulatory uncertainty that may be triggered as traditional banks increase the pace of their digital transformation or digital banks find tenable reasons to open physical branches. In Saudi Arabia, digital banks are subject to the same supervision and controls as commercial banks operating in the Kingdom, but with an added emphasis on technology, cyber security, anti-money laundering measures, tracking terrorist financing, and managing operational risks. Similarly, in Mauritius, the *Digital Banks Guideline* covers all banks licensed to conduct exclusively private banking or exclusively Islamic banking activities through digital means and also applies to both Islamic and non-Islamic digital banks without distinction. The DFSA treats any entity aiming to offer digital Islamic banking services and engage in digital Islamic banking activities similarly to other banking entities operating within the DIFC. Regardless of whether a banking entity operates digitally or through traditional means, if it provides banking services or conducts banking activities in or from the DIFC, it must comply with relevant laws, rules, and regulations. Regulatory oversight is determined based on the risks associated with the entity's operations. For instance, a "digital bank" would face additional risks related to technology and the digital delivery of services.

Some other jurisdictions focus on encouraging innovation within the financial service industry and are actively amending existing regulations to incorporate provisions for digital Islamic banking institutions. Notably, Jordan acknowledges the absence of regulation for digital Islamic banking but supports its growth. In the Philippines, Islamic banks and digital banks are treated separately but regulated under the same framework, offering flexibility and guidance tailored to their specific characteristics. In Indonesia, OJK does not make a distinction for a bank based on its business model. As such, all banks in the country have the option to operate either as a traditional or digital bank with the latter held to the additional specific regulatory requirements on risk management, governance, and contribution to the financial inclusion policy objective.

Regardless of the regulatory regime adopted, during the regulatory review process, RSAs conduct thorough evaluations considering potential unintended consequences on financial sector stability. They analyse regulatory frameworks from other jurisdictions to learn from effective practices and adapt them to their context. Both formal and informal consultations with stakeholders, including firms, industry bodies, academia, Sharīʿah scholars,

and investors help incorporate diverse perspectives into the regulatory framework. Supervisory powers and external evidence, such as research findings and reports, are employed to assess the effectiveness of existing regulations and monitor technological advancements in digital banking. Participation in test-and-learn initiatives aids in observing innovative developments during the review process.

Regulatory Approaches to Digital Islamic Banks

Phased Regulatory Regime
Malaysia
Bespoke Regulatory Regime
Pakistan
Common Regulatory Framework with some Specific Provisions
Indonesia
Common Regulatory Framework
Saudi Arabia, United Arab Emirates, Philippines, Mauritius

2.4 Complementary Regulation

Most respondents confirmed that there are complementary regulatory frameworks available that can enhance the operational efficiency of the digital Islamic banking institutions in their respective jurisdictions. These can address the opportunities and challenges arising from the evolving nature of digital banking in general and digital Islamic banking in particular. For instance, the interconnected relationships between digital Islamic banks and their numerous cloud service providers and FinTech partners have raised concerns about potential step-in risks, prompting jurisdictions to consider complementary monitoring and mitigation regulations. These complementary regulatory efforts demonstrate a commitment to embracing digital banking while ensuring customer protection, transparency, and adherence to legal and ethical standards and prioritising the stability, security, and resilience of the respective countries' financial systems.

In some jurisdictions, digital Islamic banks that are not allowed to establish a branch could use agents subject to regulators' approval. In such a case, respondents indicated that a framework for the use of intermediaries or agent banking should be established. This framework defines the roles, responsibilities, and obligations of intermediaries or agents who facilitate transactions on behalf of digital banks. It ensures that these intermediaries operate within specified guidelines, promoting efficiency and accountability in the digital banking ecosystem.

Similarly, some respondent RSAs indicated the need for a guiding framework for the relationship between a digital Islamic bank and third parties that perform outsourced services. The Central Bank of Bahrain (CBB) has introduced comprehensive guidelines through its *Operational Risk Management Module*, including regulations for outsourcing, electronic money, electronic banking, and security measures. Additionally, the establishment of a *Fintech and Innovation Unit* and a *Regulatory Sandbox* provides a controlled environment for testing innovative financial products and services.

Some jurisdictions have also developed frameworks to manage technology and cybersecurity risks. Based on responses by the RSAs, cybersecurity risk emerges as a critical concern for digital Islamic banks. Responding RSAs also emphasise the importance of enhancing data security and technological security architecture to mitigate various technological and cyber risks. Given their heavy reliance on technology and digital channels, digital banks are vulnerable to cyber threats. Therefore, robust cybersecurity measures are essential to protect customer data and financial transactions, and to maintain the overall stability of the digital banking platform. Malaysia's Bank Negara Malaysia (BNM) has released the *Risk Management in Technology* (RMiT) policy document, which outlines requirements for managing technology risk in financial institutions to ensure cyber resilience and prevent vulnerabilities. Similarly, the Central Bank of Kuwait (CBK) has taken steps to strengthen the cyber resilience of banks in its jurisdiction by issuing the *Cyber Security Framework* for the Kuwait banking sector in 2020, focusing on governance, risk management, compliance, and collaboration principles to enhance cyber resilience among banks operating in Kuwait.

Data protection is of the utmost importance in the digital banking landscape. A data protection framework is also noted as a crucial complementary framework that can be established to safeguard customers' personal and financial information. It should outline guidelines for data collection, storage, usage, and sharing, ensuring compliance with privacy regulations and protecting customers from data breaches and unauthorised access.

2.5 Regulatory Enforcement

RSAs were also asked whether regulators have the appropriate powers in their jurisdiction to take action if the activities of digital Islamic banking institutions are considered fraudulent or stray into the perimeter of such RSAs' extant regulatory activity. Although there may be no digital Islamic banks currently operating in some jurisdictions, the respective regulatory authorities maintain the power to address fraudulent activities and enforce compliance with banking laws and regulations.

In the Philippines, RSAs retain the power to take appropriate actions to address fraudulent activities or activities falling within their existing regulatory jurisdiction over banks. In Malaysia, if a licensed digital Islamic bank engages in activities that fall under the oversight of another regulator, such as capital market activities under the Securities Commission of Malaysia, the relevant regulator has the authority to take necessary actions in accordance with its mandate. Similarly, the State Bank of Pakistan (SBP) has the power to take action under relevant provisions of the law. And, the Bank of Mauritius stated that it has the ability to take actions in accordance with the powers vested in it by the Mauritian banking laws against all banks, including Islamic digital banking institutions, that are found to be non-compliant with banking laws and instructions.

In the UAE, the DFSA has the authority to take regulatory actions, including enforcement measures, if an authorised firm is involved in fraudulent activities or conducts activities beyond the scope of its license. For instance, if an authorised firm offers custody services in the DIFC without the appropriate license, the DFSA can intervene to compel the firm to cease providing such services.

The presence of an appropriate legal framework for licensing and regulation of digital Islamic banking is also seen as essential. Digital Islamic banks need a suitable environment, with a well-defined legal and regulatory framework adapted to provide Islamic financial services through digital channels.

Section 3: Prudential Considerations In Regulating And Supervising Digital Islamic Banking

Among most of the surveyed RSAs, the general view is that prudential considerations in the oversight of digital Islamic banking would largely be similar across various banking business models. Specifically, digital Islamic banks would still be required to adhere to essential capital and liquidity requirements, implement risk management frameworks, fulfil governance, disclosure, and conduct of business regulations, and ensure full Sharī'ah compliance in their operations. Nevertheless, the unique aspects of digital Islamic banking, coupled with its relatively recent regulatory establishment in many jurisdictions, necessitate a revaluation of some identified prudential matters (Appendix B).

3.1 Risk Management

One crucial area of prudential consideration for digital Islamic banks, highlighted by most RSA respondents, is risk management. Risk management should consider the particularities of a digital bank's operations and business model, encompassing technology and adherence to Sharī'ah principles. However, beyond Sharī'ah-governance requirements, no particular Islamic finance specifics were identified by surveyed members. This does not, however, preclude risks that may become apparent as the segment matures over time.

3.2 Operational Risks

Digital banks face operational risks due to their technology-driven operations. Disruptions or failures in technology systems can lead to significant operational risks, including service outages and financial losses. It is important to note that digital Islamic banks' unique business model makes operational risks more prevalent than other risks they face. These operational risks are diverse and challenging to estimate accurately due to limited data availability. However, when computing the capital adequacy ratio, operational risks are equally applicable regardless of whether it is an Islamic or conventional digital bank.

Operational risks may extend to Sharī'ah non-compliance risks (SNCR). Additional remarks from some RSA respondents indicate that SNCR could also occur indirectly due to breaches of Sharī'ah requirements or errors in the order or number of critical steps involved in a contract. For example, in commodity *murābaḥah* for Islamic personal financing, if the Islamic bank omits or improperly sequences any steps, the transaction becomes Sharī'ah non-compliant. While digitalisation can improve and expedite previously manual processes, attention to detail is necessary to ensure Sharī'ah compliance.

3.3 Capital and Liquidity Management

Capital and liquidity requirements in IFSB standards, while primarily designed for banking institutions offering Islamic financial services, may be adapted to accommodate the specificities of digital Islamic banking. The requirements for digital Islamic banks may differ across countries and encompass various risks. However, it is crucial to set these requirements at a sufficient level to absorb losses, especially during the formative years when the digital Islamic banking model is relatively untested and susceptible to market volatility. At the same time, regulatory measures should not be overly prohibitive such that

they discourage potential applicants. In Malaysia, digital banks are subject to a minimum capital requirement of RM 100 million during the first five years of operation, using the standardised approach and based on a simplified risk-weighted asset schedule. They must also meet the common equity Tier 1 threshold but are exempted from countercyclical and capital conservation buffers. After this initial phase, digital banks in Malaysia are subjected to the same prudential requirements as all other banks operating in the country. In the Philippines, the required minimum capitalisation for digital banks is PHP1.0 billion while in Pakistan, fully licensed digital banks, like their standard commercial banking counterparts, are expected to maintain a minimum capital requirement of PKR 10 billion. These variations reflect the regulatory differences across jurisdictions.

In terms of liquidity requirements, most jurisdictions, especially those already following Basel III, do not specify different requirements for digital banks, suggesting that all banks, regardless of their business model, adhere to the same liquidity standards. In Malaysia, the digital banking framework requires digital banks to hold an adequate stock of unencumbered Level 1 and Level 2A high-quality liquid assets (HQLA) equivalent to at least 25% of its total on-balance sheet liabilities during the foundational phase. Generally, the requirements related to eligibility of Level 1 and Level 2 HQLA and Liquidity Coverage Ratios (LCR) are similar to that of traditional banks. However, it is important to note that the cash flow underlying the computation of both ratios is based on forecasts, which may necessitate a detailed understanding of the business model of digital Islamic banks and requisite supervisory capacity on the part of the RSAs.

3.4 Governance and Customer Protection

Another relevant issue highlighted by some RSA respondents is the need for well-defined and developed governance structures. Some jurisdictions may require a robust IT and data governance structure to comply with complex data protection regulations. Another consideration is the need for technical knowledge of the relevant technologies as well as knowledge of Islamic finance as part of the collective fit-and-proper requirements for the Board and senior management of digital Islamic banks. IFSB standards on corporate governance and Sharīʻah governance may also be applicable to the governance of digital Islamic banks.

Data privacy and compliance risks are inherent in digital banking, as digital banks handle substantial volumes of customer data, making data privacy a paramount concern. Failure to comply with data protection regulations and industry standards can result in severe legal and reputational risks. Therefore, safeguarding customer information and ensuring compliance with relevant regulations are top priorities for regulators. Digital banks face unique customer risks, particularly when serving diverse customer bases, including unbanked and underbanked individuals. Thus, regulators recognise that proper risk assessment and customer due diligence are essential to address potential risks associated with these customer segments.

Consumer protection frameworks are also considered crucial as a complement to safeguard the interests of investors and those raising funds through digital banking platforms. This framework would often include established rules and regulations to ensure fair and transparent dealings, disclosure of risks, and protection against fraudulent practices, thereby fostering confidence and trust in the digital banking sector. Central Bank of the United

Arab Emirates (CBUAE) has issued new regulations for Stored Value Facilities (SVF) to support digital payment services. These guidelines cover licensing, financing, corporate governance, risk management, and customer protection.

3.5 Transparency and disclosure

Transparency and disclosure are vital aspects of digital Islamic banking. As such, regulators may consider whether there are any additional or specific requirements for a robust transparency and disclosure framework for digital Islamic banks, with regard to their products, services, fees, terms and conditions, and potential risks. The findings of this paper did not indicate that at present, any jurisdiction has set out additional disclosures for digital Islamic banks.

3.6 AML/CFT

Digital Islamic banking may encounter significant challenges related to Anti-Money Laundering (AML) and Combating the Financing of Terrorism (CFT), despite not being inherently more susceptible to these issues than other digital or traditional banks. The fast-paced and technology-driven nature of digital banking creates vulnerabilities that can be exploited for illicit financial activities. Concerns include the remote onboarding and identity verification process, which is prone to identity fraud. Implementing robust identity verification mechanisms is crucial to ensure customer legitimacy.

The high volume of transactions on digital banking platforms may pose AML/CFT challenges, making real-time supervisory or operational detection of suspicious activities complex. The responses also indicate some regulatory evidence that digital Islamic banks are vulnerable to AML/CFT risks and need to comply with associated extant regulations. This requires digital Islamic banks to conduct customer due diligence to maintain their integrity. While digital Islamic banks may be required to follow regulatory restrictions of having limited or no physical presence, as in the case of Malaysia and Pakistan, e-KYC solutions can emerge as being crucial in complying with regulatory requirements associated with customer identification and verification.

Islamic banks' involvement in transmitting *zakāh* collections to non-profit organizations (NPOs) may expose digital Islamic banks to FT risks, particularly if the NPOs lack proper regulation. A thorough review of AML/CFT rules for NPOs and sufficient information on the beneficiaries is necessary before distributing charity funds under *zakāh*. For instance, in Saudi Arabia, laws have been put in place to ensure that charitable contributions for humanitarian aid abroad are not abused, subjecting such contributions to approval by the Foreign Ministry, along with stringent conditions for reporting and account operation.

No significant evidence on e-KYC guidelines has been observed from jurisdictions that are covered in this paper. This could be due to the fact that this concept is in a very early stage. Malaysia has formulated an e-KYC policy and guidance on e-KYC implementation, risk management, application of artificial intelligence and machine learning, customer authentication, and technology to ensure effective AML/CFT control measures. However, e-KYC procedures designed to authenticate customer identity in financial transactions are in

most cases not specific to Islamic banking. Therefore, e-KYC guidance should be largely similar irrespective of the type of bank.

3.7 Resolution of Digital Islamic Banks

Emerging regulations for digital banks require, irrespective of the nature of services, an exit plan while operating in the foundational or transitional phase. This exit plan offers a set of recourses when the business model appears unsustainable and ineffectual. A digital bank, in its infancy, may face vulnerabilities to some unforeseen risks that may lead to business disruption and disorderly liquidation without meeting its obligations. The regulations point to the requirement to have predesigned guidance on exit triggers, governance procedures, adequacy funding and liquidity, engagement with the stakeholders, and a safety net for customers.

Less attention seems to have been given to the resolution of outsourced services, beyond requiring them to have alternative arrangements in place. As safety nets become increasingly important on the retail side, it may be timely to consider how financial regulators should collaborate with regulators in other sectors and with bankruptcy authorities to prevent systemic consequences.

One crucial consideration is the possibility that the bankruptcy of a digital bank is caused by the failure of a cloud service provider. In some cases, transferring to another cloud service provider might not be possible if the provider offers platform-as-a-service, and competitors use a different platform. Additionally, if a financial institution has a software-as-a-service-type contract, it may not technically be able to transfer the service to another provider, and there may be legal restrictions on using the intellectual property of the former provider with a new one. Moreover, due to the concentration of cloud service providers, if the failure of one provider affects several institutions, it may be unclear whether one or two alternative providers are capable of supporting all affected institutions instantly and simultaneously. In light of these challenges, there is a need for well-defined resolution frameworks, encompassing options like restructuring, mergers, acquisitions, or orderly winding down.

Resolving and recovering digital banks necessitates tailored approaches that account for their technological and operational risks. The IFSB Technical Note (TN-4) on recovery and resolution provides guidance to RSAs and related authorities to establish an effective recovery and resolution framework that is compliant with Sharīʻah principles. However, less emphasis has been placed on the resolution and recovery of digital banks, including processes and strategies to handle financial distress and ensure continued operation or orderly winding down, taking into account the peculiarity of their business model. While there are issues specific to Islamic banking resolution and recovery that differ from conventional banks, there are no significant differences that were identified by jurisdictions at this stage, in relation to recovery and resolution requirements for Islamic banks versus Islamic digital banks, barring any considerations around proportionality in applying the requirements.

Section 4: Conclusion And Recommendations

Different jurisdictions have taken varying approaches to regulation of digital Islamic banking. While some have developed bespoke regulations, others have adapted existing banking regulations to apply to digital banks, including banks operating on Islamic principles. Some jurisdictions do not yet have specific regulatory frameworks.

Among jurisdictions that have licensed digital banks, a consensus emerged that most regulatory requirements applicable to traditional banks are also applicable to digital banks. Therefore, among the RSAs that responded to the survey, no significant differences were observed in the prudential regulations that have been applied to digital banks compared to those for traditional banks.

Likewise, at this stage, none of the regulators surveyed have identified any Islamic-finance-specific risks that are distinct for digital Islamic banks, and thus, no particular differences in current practices for regulation of a traditional Islamic bank versus a digital Islamic bank. The Sharī'ah governance requirements that apply to traditional Islamic banking institutions have been applied by regulators to digital Islamic banks, with some minor exceptions, considering proportionality.

Notably, regulation of digital Islamic banking is still at a very early stage. Global regulators, including the BCBS, have not issued any specific guidelines with respect to digital Islamic banks, although the implications of digitalisation of finance for banks and supervisors is being studied.

The findings of this paper indicate that even among regulators that have already developed frameworks for digital Islamic banking, digital Islamic banking is still at an early stage. Therefore, it may not be possible at this stage to assess the appropriateness and effectiveness of the current frameworks. As more digital Islamic banks become operational, specific regulatory and supervisory issues and challenges may become more evident over time. Thus, regulators and other policy makers should continue to monitor the effectiveness of existing regulatory frameworks and identify any gaps to ensure that risks inherent to the business model of digital Islamic banks are adequately addressed.

It may also be important to consider that any regulatory divergences between digital and traditional banks, as well as between conventional and Islamic digital banks, or any forbearance of regulations, should only be based on the particular risks faced or linked closely with policy objectives. The findings of the paper indicate that most jurisdictions currently apply similar regulatory frameworks to both digital and traditional banks, with very minor exceptions or forbearances provided (the latter particularly applicable to the phased approach).

APPENDIX A

List of Respondents to the Survey on Regulatory Practices for Digital Islamic Banking

S/N	Regulatory and Supervisory Authorities
1	Bangko Sentral ng Pilipinas
2	Bank Negara Malaysia
3	Bank Mauritius
4	Banking Regulation and Supervision Agency Turkey
5	Central Bank of Bahrain
6	Central Bank of Libya
7	Central Bank of Sudan
8	Dubai Financial Services Authority
9	Maldives Monetary Authority
10	State Bank of Pakistan
11	Saudi Central Bank
12	Central Bank of Oman
13	Central Bank of Jordan

APPENDIX B

Comparison of regulatory and prudential requirements by selected countries that have specific regulations for digital banks.

Regulatory and Prudential Considerations	Countries	Requirements
Capital and Liquidity	**Malaysia**	During the foundational phase of 3-5 years, a licensed digital bank maintains a minimum of RM100 million at all times. A licensed digital bank shall maintain Total Capital Ratio of 8% with Common Equity Tier-1 (CET1) being the only eligible regulatory capital. A licensed digital bank shall hold high-quality liquid assets at least 25% of total on-balance-sheet assets.
	Pakistan	The minimum required capital for digital retail banks (DRB) ranges from PKR 1.5 billion to PKR 4.0 billion depending on the stages of operations and for digital full bank (DFB) ranges from PKR 6.5 billion and PKR 10.0 billion depending on the stages of operations.
	Mauritius	In the restricted phase,[12] a digital bank commences and maintains operations with stated or assigned capital of not less than 200 million Mauritian rupees or equivalent eligible assets. At the end of the restricted phase, the minimum capital requirement applicable shall be 400 million Mauritian rupees and equivalent eligible assets.
	Philippines	Minimum capitalisation of digital banks is PHP 1.0 billion.
Consumer/Customer Protection	**Malaysia**	Require an independent external assurance on internal control and IT systems complying with regulatory standards on consumer protection.
	Pakistan	Require that digital banks become members of the Deposit Protection Corporation (DPC) and meet the requirements to pay the premium as per instructions and regulations issued by DPC.
	Mauritius	Inform all customers of the restrictive phase of the digital bank and inform and educate the customers about the financial products and services and the associated security measures.
	Philippines	Follow all prudential requirements set out by BSP on consumer protection.
Resolution plan	**Malaysia**	At the time of application, submission of an exit plan for the first five years of operation with foreseeable management triggers and solid governance to ensure orderly wind-down or transfer of business.
	Pakistan	Establishment of an exit plan, involving a plan for portfolio exit and liquidation of the bank, providing adequate protection for customer/depositors' interests and setting prudential thresholds or alerts.
	Mauritius	Submit an exit plan at the time of application, demonstrating channels and sources of funds to have significant shareholders compensate depositors in case of a shortage of assets to cover the deposit liabilities.
Shari'ah Governance	**Malaysia**	Comply with Shari'ah Governance policy with some relaxation on forming the Shari'ah committee and the number of Shari'ah committee meetings in a year.
	Pakistan	Follow Shari'ah governance and its principles applicable to traditional Islamic banks for digital product offerings and any changes therein.
AML/CFT	**Malaysia**	Follow Regulatory requirements applicable to the licensed Islamic banks.

[12] The restricted phase shall comprise a mobilisation period of not more than two years and a subsequent transitional period of not more than three years. There are several restrictions imposed on the activities of the digital bank during the restricted phase.

		Secure an independent external assurance on internal control and IT systems complying with regulatory standards on AML/CFT.
	Pakistan	Comply with AML/CFT and associated requirements applicable to commercial banks in general (conventional or Islamic as the case may be).
	Mauritius	Comply with the relevant statutory and regulatory requirements relating to AML/CFT issued by Bank of Mauritius with additional requirements to follow internal policies, procedures, and controls through compliance management arrangement, including the appointment of a compliance officer at the management level.
	Philippines	Follow all prudential requirements set out by BSP on AML/CFT.
Data protection/Cyber security	**Malaysia**	Secure an independent external assurance on internal control and IT systems complying with regulatory standards on cyber security.
	Pakistan	Ensure at least one board member has adequate knowledge on cyber security, cloud storage, advanced data, and analytics. Follow existing requirements concerning technology, cloud storage, and cyber security applicable to Islamic banks.
	Mauritius	Comply with relevant data protection laws and regulations. Ensure and implement appropriate and robust cyber and technology risk management framework.
	Philippines	Follow all prudential requirements set out by BSP on Information Technology and cyber security.

Note: *Only four countries have been found to have separate regulatory documents on digital banking. Regulatory and prudential requirements are extracted from the respective regulatory documents,13 survey responses, and interviews with RSAs.

**For the Philippines, Islamic banks and digital banks are two separate and distinct categories of banks along with five other categories and are regulated under a single framework. Only those granted Islamic banking licenses have the powers necessary to carry out the business of a bank in accordance with Sharī'ah principles. However, banks licensed for Islamic banking can offer products and services via digital platforms. So, Sharī'ah governance is not applicable to digital banks.

[13] Licensing Framework for Digital Banks, Bank Negara Malaysia (2020), Licensing and Regulatory Framework for Digital Banks, State Bank of Pakistan (2022), Guideline for Digital Banks, Bank of Mauritius (2021), and Circular No. 1154, Bangko Stntral Ng Pilipinas (2022).

REFERENCES

Adewale, A. A., & Ismal, RI (2020), IFSB Working Paper Series - Digital Transformation in Islamic Banking. December. http://www.ifsb.org/docs/WP-03-Consumer Protection(final).pdf

Bank Negara Malaysia (2020), Licensing Framework for Digital Banks. Bank Negara Malaysia, December, 27. https://www.bnm.gov.my/index.php?ch=57&pg=137&ac=924&bb=file

Bank Of Mauritius (2021), Guideline for Digital Banks. December. https://www.bom.mu/sites/default/files/guideline_for_digital_banks_06.12.2021.pdf

Bangko Stntral Ng Pilipinas (2022), Circular No. II54. https://www.bsp.gov.ph/Regulations/Issuances/2022/1154.pdf

Erdemir & Özmen Attorney Partnership (2021), Draft Regulation on the Operating Principles of Digital Banks and Banking as a Service.

State Bank of Pakistan (2022), Licensing and Regulatory Framework for Digital Banks. http://www.ifsb.org/docs/WP-03-Consumer Protection(final).pdf