IFSB WORKING PAPER SERIES

WP-19/12/2020

DIGITAL TRANSFORMATION IN ISLAMIC BANKING

December 2020

ISLAMIC FINANCIAL SERVICES BOARD

IFSB WORKING PAPER SERIES

Technical and Research Department

WP-19/12/2020

DIGITAL TRANSFORMATION IN ISLAMIC BANKING

Abideen Adeyemi Adewale Rifki Ismal

December 2020

Corresponding email: research@ifsb.org

This working paper has benefited greatly from the feedback and guidance provided by a core team from the Technical and Research Department of the IFSB Secretariat. The authors would like to acknowledge the immense contribution of the members of the IFSB Technical Committee who reviewed and approved the paper. Mrs. Ida Shafinaz Ab. Malek, Ms. Fadhila Izzati Mokhtar, and Ms. Nur Khairunissa Md Zawawi, of the IFSB Secretariat provided support in distributing the survey to the IFSB member institutions, and Ms. Rosmawatie Abdul Halim assisted with the formatting and publishing of the paper, respectively. Finally, the authors are grateful to the regulatory and supervisory authorities that provided useful comments on the draft paper during IFSB members' consultation. Many thanks to the Islamic banks from various jurisdictions for their participation in the survey,

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 of 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**.

GLOSSARY

ʻAqd	An agreement between two willing parties to initiate, adjust or terminate a given transaction in a manner binding upon both parties.
Commodity *Murābaḥah*	A murābaḥah transaction based on the purchase of a commodity from a seller or a broker and its resale to the customer on the basis of deferred *murābaḥah*, followed by the sale of the commodity by the customer for a spot price to a third party for the purpose of obtaining liquidity, provided that there are no links between the two contracts.
Hibah	The payment of money or transfer of an asset to another party without a consideration.
Ijārah	A contract made to lease the usufruct of a specified asset for an agreed period against a specified rental. It could be preceded by a unilateral binding promise from one of the contracting parties. The *ijārah* contract is binding on both contracting parties.
Muḍārabah	A partnership contract between the capital provider (*rabb al-māl*) and an entrepreneur (*muḍārib*) whereby the capital provider would contribute capital to an enterprise or activity that is to be managed by the entrepreneur. Profits generated by that enterprise or activity are shared in accordance with the percentage specified in the contract, while losses are to be borne solely by the capital provider unless they are due to misconduct, negligence or breach of contracted terms.
Murābaḥah	A sale contract whereby the institution offering Islamic financial services sells to a customer a specified kind of asset that is already in its possession, whereby the selling price is the sum of the original price and an agreed profit margin.
Mushārakah	A contract between the institution offering Islamic financial services and a customer whereby both would contribute capital to an enterprise, whether existing or new, or to ownership of real estate or a movable asset, on either a temporary or a permanent basis. Profits generated by that enterprise or real estate/asset are shared in accordance with the terms of the *mushārakah* agreement, while losses are shared in proportion to each partner's share of capital.
Qarḍ	The payment of money to someone who will benefit from it provided that its equivalent is repaid. The repayment of the money is due at any point in time, even if it is deferred.
Sharīʿah	The practical divine law deduced from its legitimate sources: the Qur'ān, Sunnah, consensus (*ijmāʻ*), analogy (*qiyās*) and other approved sources of the Sharīʻah.
Sharīʿah Board	An independent body set up or engaged by the institution offering Islamic financial services to supervise its Sharīʻah compliance and governance system.
Sharīʻah Non-Compliance Risk	An operational risk resulting from non-compliance of the institution with the rules and principles of Sharīʻah in its products and services.
Ṣukūk	Certificates that represent a proportional undivided ownership right in tangible assets, or a pool of tangible assets and other

	types of assets. These assets could be in a specific project or specific investment activity that is Sharīʿah-compliant.
Wadīʿah	A contract for the safekeeping of assets on a trust basis and their return upon the demand of their owners. The contract can be for a fee or without a fee. The assets are held on a trust basis by the safekeeper and are not guaranteed by the safekeeper, except in the case of misconduct, negligence or breach of the conditions.

Abstract

This exploratory working paper investigates the activities relating to the digital transformation process of Islamic banks (IBs). Data elicited via a survey questionnaire from 80 IBs across 21 Islamic Financial Services Board member jurisdictions were subjected to descriptive analysis to investigate the IBs' rationales for digitalisation, as well as their current status and the technologies they have adopted. The paper also investigates the regulatory approaches, challenges, prudential risks and financial stability implications of digitalisation of Islamic banking. The paper found that in most IBs the digitalisation process is still in progress but has gained more traction since the outbreak of the COVID-19 pandemic. Among many other pertinent reasons cited in the paper, strengthening competitiveness, enhancing operational efficiency and improving customer satisfaction are the main rationales for IBs' digitalisation drive. The technologies adopted include mobile and digital wallets, biometric authentication and artificial programming interface. Notwithstanding, IBs' digitalisation drive has been impeded by legacy infrastructure, and by the lack of both the requisite human resources and an open banking infrastructure and architecture. The paper examines the implications of the benefits and the risks of digitalisation for the stability of the Islamic banking industry and makes recommendations on the way forward.

Table of Contents

SECTION 1: INTRODUCTION

1.1 Background

The adoption of innovative technologies and business models is a prominent emerging trend that is fast changing the ecosystem of the Islamic Financial Services Industry (IFSI), and the Islamic banks (IBs) are not immune to these developments. Prior to the outbreak of the COVID-19 pandemic, digitalisation in the Islamic banking industry has been building momentum and increasingly transforming the financial products offered and services rendered. As many countries were entering the recovery phase of the first wave of the pandemic, a second wave was recorded and subsequently compounded by the discovery of a new and more infectious mutation of the SARS-CoV-2 virus.[1] The consequential reintroduction of the movement restrictions and physical distancing as measures to flatten the curve of the spread of COVID-19 has also added speed to the need for digital transformation in rendering financial services.

Digital transformation is crucial in order to sustain the growth momentum of the Islamic banking industry[2] by broadening its current outreach, exploring new horizons, identifying untapped potentials, and unlocking opportunities especially in financially developed markets but with minimal or no presence of Islamic banking.[3] To achieve this, a radical departure is required from the traditional sales and product-inclined Islamic banking model to a collaborative, or competition-induced innovative model of Islamic banking and financial service delivery. Such model should align with the high expectations of today's tech-savvy and convenience-driven customers[4] whose digital banking behaviours have also been evolving in parallel.

Digitalising Islamic banking will bring about a myriad of opportunities for the growth of the industry. For instance, it will help IBs to respond to changing customer structure and expectations as well as to the consequential disintermediation due to competition from new-entrant non-bank Islamic financial services providers. Richer insights will be put into business decision-making due to availability and processing of more granular data about customers preferences and disposition. Digitalising Islamic banking will also enhance access to financing by the micro, small and medium enterprises (MSMEs),[5] and support value-based intermediation[6] among offering many other benefits.

Digitalisation will enhance IBs' compliance with regulatory requirements and risk management capabilities. Moreover, supervisory activities and capabilities of the regulatory and supervisory authorities (RSAs) would be enhanced due to the resultant operational efficiency and effectiveness brought about by automation of supervisory processes, improved real-time data capture and use. RSAs have also been able to strengthen their consumer protection role by

---

[1] Severe acute respiratory syndrome coronavirus 2 (SARS-CoV-2) is the strain of coronavirus that causes coronavirus disease 2019 (COVID-19), the respiratory illness responsible for the COVID-19 pandemic.

[2] As per the IFSB's *Islamic Financial Services Industry (IFSI) Stability Report 2020*, the Islamic banking industry recorded a y-o-y growth of 12.7% in 2019. It is now worth USD 1.77 trillion, accounting for 72.4% of global worth of the Islamic financial services industry, and is of systemic importance by accounting for more than 15% share of domestic banking assets, in 13 jurisdictions.

[3] For instance, Insha, a spin-off start-up of Albarka Türk Participation Bank is an Islamic digital-only bank which is based in Germany. As at October 2020, the digital only bank which was launched in 2018 hit 40,000 users in Germany and aims to expand its activities to other parts of Europe where a sizeable number of potential Muslim clients reside. https://www.salaamgateway.com/story/german-islamic-fintech-insha-releasing-new-app-in-july-eyes-europe-expansion.

[4] pwc (2019) Virtual Banking: Malaysian Customers Take Charge. https://www.pwc.com/my/en/assets/workshops/2019/virtual-banking-malaysian- customers-take-charge-report.pdf.

[5] According to the International Finance Corporation (IFC), 65 million or 40% of formal MSMEs in developing countries have annual unmet financing need of USD 5.2 trillion. https://www.worldbank.org/en/topic/smefinance

[6] Bank Negara Malaysia, for instance, is at the forefront of this proposition of value-based intermediation. https://www.bnm.gov.my/index.php?ch=en_speech&pg=en_

leveraging on technology to augment their consumer complaints management system through, for instance, a chatbot application for complaints handling.[7]

Digitalisation also promotes financial inclusion in line with the agenda of development finance institutions, regulators, standard setters and other institutional stakeholders in the financial services industry.[8] In this regard, the positive implication of digital Islamic banking for financial inclusion is also noteworthy and in line with global trend as highlighted by the IFSB.[9] This is due to the structural composition and dynamics of the traditional and potential customer base of the IBs. The median age of Muslims worldwide is 24 years compared to 32 years globally. Fifteen among the top 59 countries with smartphone penetration are Organisation of Islamic Cooperation (OIC) member countries. Compared to 49% worldwide, 72% of the unbanked population reside in the OIC countries.[10]

Notwithstanding its numerous benefits, digitalisation may also create exposure to potential risks that have implications for the financial stability and integrity of the Islamic banking industry.[11] Such may derive from how the incumbent IBs respond to the challenges arising from both market structure dynamics, risks and challenges involved in transformation to digital Islamic banking.

Digitalisation may also expose IBs to cyber-security risk, data quality issues, money laundering and financing terrorism (ML/FT) risks, and cloud-concentration risk. Consumers and investors may also be exposed to protection issues. Sharīʿah non-compliance risks could also result from the special intricacies of the Islamic banking products and processes in the event of non-compliance with the essentials and sequence of automated Sharīʿah requirements due to programming error or system malfunctioning.

The regulatory implications of digitalisation would depend on RSAs' response to finding a balance between encouraging technology-based financial innovation while protecting consumers,[12] supporting business operations, and promoting financial inclusion. This should be done without infringing on the fundamental premise of Sharīʿah[13] upon which Islamic banking is built. In this regard, RSAs have also been issuing guiding frameworks and regulations, promoting regulatory sandboxes and the establishment of digital banking institutions including for Islamic banks.

Across IFSB jurisdictions, IBs are in different stages of development and implementation of activities relating to the digital transformation of Islamic banking operation. Some IBs are already deploying technology in their operation via the use of software applications, especially

[7] Bangko Sentral ng Pilipinas (BSP) is a pioneer RSA in this regard. https://static1.squarespace.com/static/583ddaade4fcb5082fec58f4/t/5c62711941920237ef03d090/1549955392920/R2A+Chatbot+Case+Study.pdf

[8] Regulators Consider Benefits, Challenges of Digital Financial Inclusion. 11-minute feature video produced by GPFI/CGAP. https://www.youtube.com/watch?v=JTSb61PGrpM&feature=youtu.be

[9] IFSB's *TN-3: Technical Note of Financial Inclusion and Islamic Finance* 2019. https://www.ifsb.org/download.php?id=5519&lang=English&pg=/published.php

[10] *Islamic Fintech Report 2018: Current Landscape & Path Forward.* https://www.dinarstandard.com/wp-content/uploads/2018/12/Islamic-Fintech-Report-2018.pdf

[11] FSB (2019), *FinTech and Market Structure in Financial Services: Market Developments and Potential Financial Stability Implications*, p. 1: www.fsb.org

[12] The OECD has stated that, due to the risks of digital financial services, vulnerability of consumers to unfair and deceptive practices may increase. See: OECD (2018), *G20/OECD Policy Guidance on Financial Consumer Protection Approaches in the Digital Age*, p.14.

[13] Forty per cent of Islamic FinTechs are already Sharīʿah certified, while another 4% and 32% are either in the process of obtaining Sharīʿah certification or intend to seek certification in the future, respectively. https://ceif.iba.edu.pk/pdf/IslamicFinTechReport19.pdf

for payments and transaction services and remote customer on-boarding[14]. Other IBs are adopting robotics process automation, machine learning and artificial intelligence (AI) technology for repeatable transactional tasks. Some IBs have also deployed predictive analytics based on big data, cloud computing and the Internet of Things (IoT) to better anticipate customer needs. Similarly, unbundling of services and data sharing in open banking applications[15] are being implemented via application programming interfaces (APIs).[16]

This paper investigates the digital transformation process in the Islamic banking industry. The scope of the paper covers only IBs in Islamic Financial Services Board (IFSB) member jurisdictions. Given the exploratory nature of the research, except to enhance the explanation no inferences are drawn, and no preferences are indicated for any of the numerous technology-driven financial innovations mentioned in the paper. Rather, a general overview is provided of the situation and the pertinent prudential issues.

1.2 Objectives

The specific objectives of this working paper include to investigate:

- the current status of digital transformation among IBs in various IFSB jurisdictions;
- the peculiar impediments or challenges to its implementation in various IFSB member jurisdictions;
- the prudential risks that may crystallise from digitalisation of Islamic banking operation;
- the implications of digitalisation for the financial stability of the Islamic banking industry;
- what needs to be done to support the digital transformation process in Islamic banking.

1.3 Methodology

The data used in this study were collected via questionnaire survey distributed online. The survey was addressed to IBs via the RSAs in various IFSB member jurisdictions between September and October 2020.[17] The survey comprised mainly closed-ended questions with codes to indicate options a respondent IB might wish to select. In some other instances, open-ended questions were also included for the respondents IBs to freely express their opinion on related matters beyond the closed-ended options provided.

The cooperation of the responding IBs was sought especially in terms of ensuring 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 elicited from 80 Islamic banks cutting across 21 IFSB member jurisdictions[18] were subjected to descriptive data analysis only, mainly

[14] A notable example is the Roshan Digital Account, which is an initiative of the State Bank of Pakistan in collaboration with commercial banks operating in Pakistan. It provides opportunities for the non-resident Pakistanis to undertake various financial activities like banking, investment, payment etc. in Pakistan. https://www.sbp.org.pk/RDA/index.html

[15] According to the Financial Stability Board (FSB) (2019), "open banking operations" refers to a system in which financial institutions' data can be shared with users and third-party developers through APIs: *FinTech and Market Structure in Financial Services: Market Developments and Potential Financial Stability Implications*: www.fsb.org.

[16] APIs connect software programmes and allow them to communicate based on programming code. See: State of the Global Islamic Economy Report, 2018/2019, p. 18. https://haladinar.io/hdn/doc/report2018.pdf

[17] The survey was also distributed directly to Islamic banks that are observer members of the IFSB.

[18] The list of the IFSB member jurisdictions and number of IBs that responded to the survey is provided in the appendix.

based on simple percentage, frequency and, in one instance, weighted-mean scores to show relative importance.[19]

This paper is divided into six sections. In the remaining sections, the survey results obtained are analysed with reference made to the extant related literature. Section 2 focuses on the current status and rationale for digitalisation in IBs. Section 3 examines the technological advancements adopted by IBs and the various prudential risks they are faced with in their digital transformation process. Section 4 focuses on regulation and the impediments to digital transformation of Islamic banking, and Section 5 on the implications of digital transformation for the stability of the Islamic banking industry. The final section presents conclusions and recommendations.

SECTION 2: CURRENT STATUS OF AND RATIONALE FOR IB's DIGITALISATION

2.1 IBs' Perceptions of Digitalisation

The first survey question asked the respondent IBs about what they perceive digital Islamic banking to be in the context of their operations. The responses provided generally fits into the definition of digital financial services (DFS) provided by the Organisation for Economic Cooperation and Development (OECD)[20] which states that:

> *DFS involves financial operations using digital technology, including electronic money, mobile financial services, online financial services, i-teller and branchless banking, whether through bank or non-bank institutions. DFS encompass various monetary transactions such as depositing, withdrawing, sending and receiving money, as well as other financial services, including payment, credit, pensions and insurance. DFS can also include non-transactional services such as viewing personal financial information through digital devices.*

Some of the responding IBs view digitalisation of their operations from the perspective of what Islamic banking products and services they offer. Some others extend such views to include the various channels or platforms through which such services are offered to their customers. Some IBs also view digitalisation of their Islamic banking activities as enhancements to their operational efficiency, data security, regulatory compliance, and customer experience in its entire ramification via technology.

A noteworthy response offered by some IBs is that such digital operation is performed on the basis of the permissibility offered by their operating license. As such, a digital Islamic bank is that which is duly licensed by the relevant RSA to provide all traditional banking and intermediation services while leveraging on the latest technological advancements to improve its banking model. This could be in the form either as a fully digital retail bank, marketplace bank, or offering Banking-as-a-Service.[21] Such digital Islamic bank is therefore, different from an Islamic neobank which though may offer Islamic financial services via technology is not

[19] The analysis is based on pooled data which may conceal jurisdictional or institutional peculiarities. This concern is addressed in some instances in this paper in cases where such a peculiarity is considered material and relevant information is available.
[20] OECD (2018), *G20/OECD Policy Guidance on Financial Consumer Protection Approaches in the Digital Age*, p. 13.
[21] A fully digital bank leverages on technology to offer enhanced banking experience at a reduced cost. A marketplace bank is essentially created by an existing licensed bank as a one-stop centre to enhance easy accessibility to its various products and services in response to competition from start-ups. Banking-as-a-Service model is usually adopted by existing technology companies that though have been duly licensed to offer banking services view banking as market utilities. Jenik, I, Flaming, M, and Salman, A. (2020) *Inclusive Digital Banking: Emerging Case Markets Case Studies*, CGAP/World Bank https://www.cgap.org/sites/default/files/publications/2020_10_Working_Paper_Inclusive_Digital_Banking.pdf

licensed to perform financial intermediation services. Perhaps, neobanks in their bid to avoid regulation and compliance cost would not opt to become licensed digital banks, so would not be able to venture into activities like accepting deposits.

Regardless of the form or business model a digital IB takes, a notable common statement among the respondent IBs is that Sharīʿah-compliance must nonetheless be ensured. Though digitalisation universally reflects the application of new technology to improve the processes, products and business models used in rendering financial services, Islamic banking digitalisation would require something more for it to be conceptually, practically, and justifiably different.

Such difference may be hinged on the fact that while technological innovation is important to Islamic banking, it should not also provide a premise upon which the principles of Sharīʿah would be compromised. As such, Islamic banking digitalisation addresses in addition to those faced by conventional banks, Sharīʿah non-compliance matters that may arise from product design and service delivery based on technology. This is in a manner that permits a discerning end-to-end Sharīʿah compliance in contractual relationships, rights and beneficial ownership, products and services offerings, marketing, etc.

2.2 Rationales for Islamic Banking Digitalisation

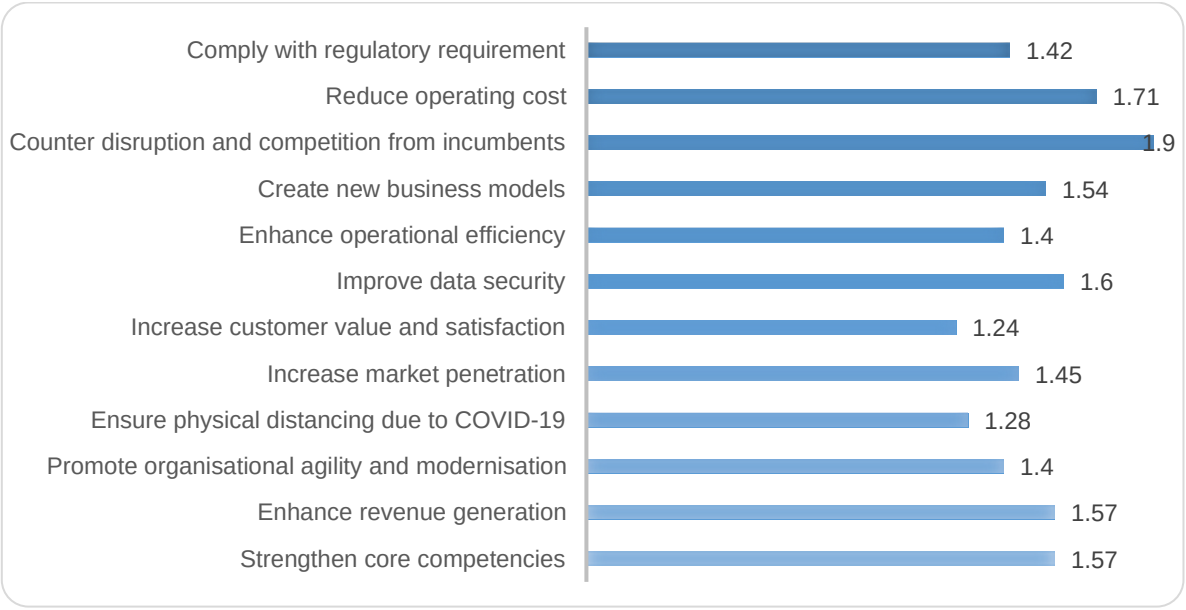
The next question in the survey sought the responding IBs' rationale for embarking or proposing to embark on digital transformation. Across jurisdictions, customer satisfaction is considered a key rationale for digital transformation in Islamic banking. Specifically, other key rationales are moderated by systemic significance of domestic Islamic banking sector, and structural and geographical factors.

Competition and contestability are considered very pertinent among IBs in jurisdictions that have attained systemic importance. IBs from some of these jurisdictions also consider compliance with regulatory requirements as a key rationale for their digital transformation activities. Whereas, in jurisdictions with very marginal share of domestic Islamic banking asset and large population, market penetration and cost reduction are considered prime rationale for most IBs' digital transformation. The COVID-19 outbreak has also added impetus to digitalisation process among IBs from these latter jurisdictions. Most IBs from the Gulf Cooperation Council (GCC) region, Bangladesh and Pakistan consider improvement in data security as key.

Based on the literature review, 12 possible reasons why IBs should engage in digital transformation were listed in the survey questionnaire. Participants' responses indicated that all the reasons stated are considered pertinent. In order to determine the relative importance of each of these stated reasons, a weighted mean analysis[22] is conducted and the outcome is depicted in Figure 2.1.

[22] The data from the questionnaire in relation to this and similar questions were generated on a scale of 1 to 5. In isolation and at varying percentages, responses to all 12 items were indicated as either "Strongly Agree" or "Agree", except in a few instances when the "Neutral" option was indicated. Explaining each item would require many tables to indicate what percentage is "Strongly Agree = 5", "Agree = 4", "Neutral = 3", "Disagree = 2", or "Strongly Agree = 1". However, the interpretation reflected in Figure 2.1 is based on weighted scores. The figures are absolute and are interpreted based on their degree. Each item is given an equal weight of 1, then multiplied by responses obtained from each IB respondent.

Figure 2.1 Reasons Why IBs Engage in Digital Transformation



Source: IFSB Survey, 2020

Specifically, with a weighted mean score of 1.9, the IBs generally consider countering disruption by new entrants and competition from other incumbent IBs as a relatively most pertinent justification for embarking on digital transformation. Both competition and competitors are changing, and IBs will need to respond accordingly. Competitive differentiation and contestability of the IBs will largely depend on to what extent they can digitalise their workplaces. This is crucial to enhance operational efficiency through optimal combination of both front-office and back-office technology, as well as to attract the right talents with the specific requisite human capital.

Competition and contestability are envisaged to further increase as new players come on board and regulators respond to finding a balance between encouraging innovation, protecting consumers[23] and ensuring financial stability.[24] The responses obtained, therefore, seems more of a pre-emptive justification than contingent reaction to threat from both FinTechs and BigTechs.[25] This is because, at the moment, both large and small IBs consider competition from the novel and technology-enabled business model of the new entrants as being moderate at most.[26] As shown in Figure 2.2, only 32%[27] of the respondent IBs, "strongly agree" that competition from new entrants when considered in isolation, is a reason for their digitalisation process. These IBs are mainly from nine systemically important and one non-systemically important Islamic banking jurisdictions.[28]

[23] The OECD has stated that, due to the risks of digital financial services, vulnerability of consumers to unfair and deceptive practices may increase. See OECD (2018), *G20/OECD Policy Guidance on Financial Consumer Protection Approaches in the Digital Age*, p. 14

[24] X. Vives (2019), "Digital Disruption in Banking", *Annual Review of Financial Economics*, Vol. 11, p. 243. Hereafter "Vives (2019)"

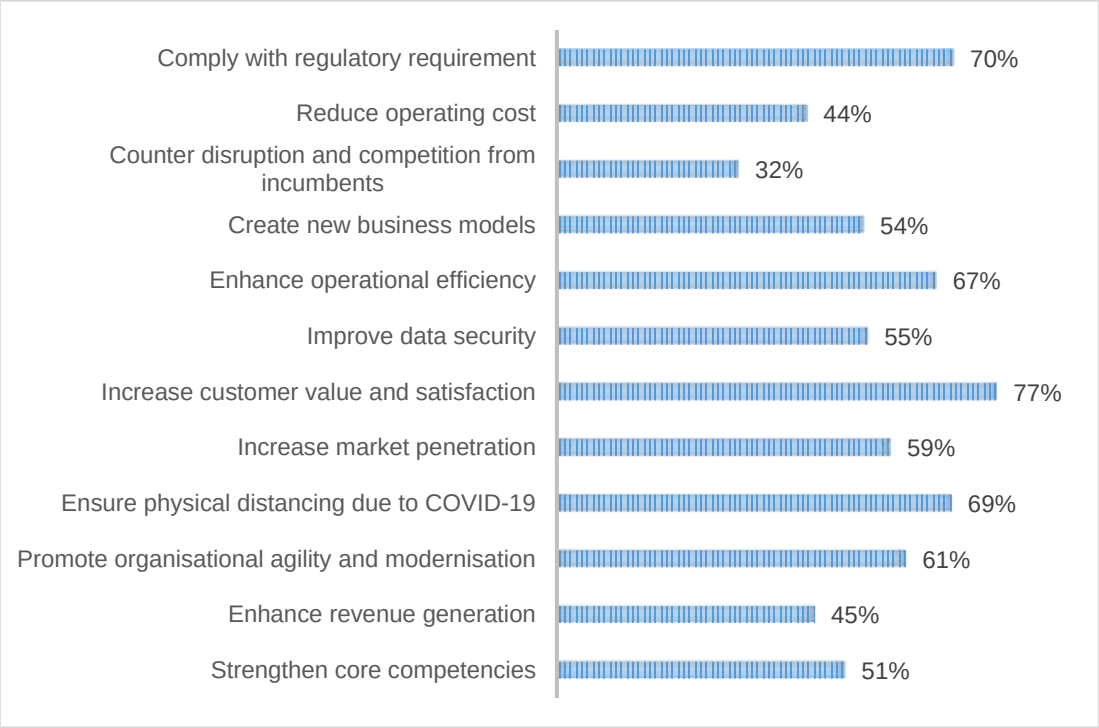
[25] FinTechs are "technology-enabled innovations in financial services that could result in new business models, applications, processes or products with an associated material effect on the provision of financial services". BigTechs are firms leveraged on their technological advantage, and on their possessing data about a large number of their pre-existing customer base, while rendering their primary business. On the basis of these dual advantages, they add rendering financial service to their value chain. FSB (2019), *FinTech and Market Structure in Financial Services: Market Developments and Potential Financial Stability Implications*

[26] General Council for Islamic Banks and Financial Institutions (CIBAFI), Global Islamic Bankers' Survey, 2019: *Sustainability, Growth Drivers, and the Regulatory Challenge*: http://cibafi.urbansoft.co.uk/Files/L1/Content/CI1809-CI1809-GlobalIslamicBankersSurvey2019Report.pdf

[27] This increases to 78% if IBs that indicate that they 'agree' are considered.

[28] The systemically important Islamic banking jurisdictions include: Bahrain, Bangladesh, Brunei, Jordan, Kuwait, Malaysia, Pakistan, Saudi Arabia and the United Arab Emirates. The non-systemically significant Islamic banking jurisdiction is Indonesia.

Figure 2.2. Proportion of IBs that "Strongly Agree" with Reasons for Digitalisation



Source: IFSB Survey, 2020

Customer satisfaction is a very important rationale for IBs' engaging in digital transformation in today's customer-centric financial market. Customer satisfaction as an important reason for digitalisation recorded a weighted-mean-score of 1.24 as shown in Figure 2.1, with 77% of the respondent IBs[29] also indicating that they "strongly agree" with this view considered in isolation as shown in Figure 2.2. Customers not only want improved services at a lower cost but also more conveniences in their banking experiences. The future outlook of the financial system revolves around the repository and availability of, and access to accurate yet comprehensive digitalised data about a customer. Such data are expected to be processed in real-time based on algorithms to arrive at customers' credit worthiness, insurance or investment preferences.

Simplification of banking processes and added convenience via technology have resulted in customer satisfaction, which has positive implications for banks' economic bottom lines. Changing customer demand particularly from the increasing number of millennials who have grown up in a digitally connected world and do not have the same loyalty to banks as older generations is adduced as one of the factors driving the prominence of digitalisation. While some consumers, particularly corporates, remain loyal to banks, changing retail consumer expectations are exerting pressure on banks to adopt various forms of technology to improve their services. This has brought about value given that customers now have more access to hitherto restricted assets, more control of their choices, and more visibility in product development.

The responding IBs also indicate the need to reduce operating costs with a weighted-mean score of 1.71. As shown in Figure 2.2, 44% of the IBs "strongly agree" that cost reduction is a reason to embark on digital transformation. Most of these IBs are from jurisdictions with a very

[29] Except respondent IBs from both Malaysia and Turkey.

small domestic Islamic banking sector but with huge Islamic banking markets.[30] It has become inevitable for IBs in these jurisdictions to replace legacy infrastructures to enhance their competitiveness and operational efficiency. Digitalisation would confer outreach opportunities on adopting IBs especially in these jurisdictions to extend services to underserved areas at a lower cost and without opening more branches.

Perhaps due to their relative operational efficiency, some IBs mainly from jurisdictions that have systemically important Islamic banking sector like Bahrain, Brunei, Malaysia, Pakistan, Saudi Arabia, and UAE indicate cost reduction as one of the least reasons for digitalisation. As indicated later on in this paper, there has been a gradual shift over time among IBs from these jurisdictions from an on-premises data service to a public cloud-based data service. The possibility of technology externalisation due to the proliferation of technology vendors and platforms that offer cloud services have perhaps significantly reduce the IBs' infrastructure and human resource requirement costs.

The need to comply with regulatory requirements is indicated by respondent IBs with a weighted-mean score of 1.42. As shown in Figure 2.2, 70% of the IBs "strongly agree" that it is a reason to embark on digital transformation. Most of these IBs are from jurisdictions with existing regulations specifically for digital banking, or regarding various other aspects related to digital banking like collaborating and partnering with FinTechs, outsourcing of cloud services, risk management in technology, cyber security, regulatory sandboxes etc.[31]

Improvement in data security and technological security architecture to mitigate against various forms of technological and cyber risks is also indicated as being very important by the responding IBs. With a weighted-mean score of 1.60, IBs, mostly from the GCC countries, Pakistan, and Bangladesh indicate that issues of data privacy and integrity are on the front burner. The response from the Bangladesh IBs is perhaps influenced by previous experience of cyber-attack on the Bangladesh Bank in 2016, and the warning of a potential cyber-attack on the country's banking system amid a 12.6% surge in internet banking since the outbreak of the COVID-19 pandemic.[32]

The response from the GCC is due to the high exposure to cyber-attack[33] given the relatively advanced deployment of digital technology for financial services in the region with various countries embarking on policies to unlock the possibilities offered by Big Data, transform key cities within the region to smart cities, and increase the use of blockchain transactions.[34] In fact, the Central Bank of Kuwait issued a cyber-security framework in 2020 to strengthen the cyber-resilience of Kuwait banking sector in the wake of growing frequency and sophistication of cyber-attacks.[35]

More than half, specifically 55% of the respondent IBs also "strongly agree" that improvement of data security is pertinent. In the event of a data breach either through theft, disruption, or damage, the reputation of an IB and the confidence of the general public and customers in particular in the deployed technology may be significantly affected.

[30] These include Indonesia, Morocco, Nigeria, Senegal, and Sri-Lanka. Although with a systemically significant Islamic banking sector, the IBs from both Jordan and Sudan also indicate strong agreement that cost reduction is a pertinent reason for their digital transformation process.
[31] These include Bahrain, Bangladesh, Egypt, Indonesia, Jordan, Kuwait, Kyrgyz Republic, Pakistan, Malaysia, Saudi Arabia, Turkey and UAE.
[32] https://tbsnews.net/economy/banking/bangladesh-bank-warns-banks-fresh-cyber-attack-amid-pandemic-128431
[33] https://www.khaleejtimes.com/business/local/over-50m-cyber-attacks-recorded-in-gcc
[34] https://castlereagh.net/developing-cyber-resilience-the-gccs-approach/
[35] https://www.cbk.gov.kw/ar/images/csf-feb-2020-1_v00_tcm11-148304.pdf

Other reasons recorded weighted-mean scores around the average of 1.51, as shown in Figure 2.1. For instance, creating new business models, and promoting organisational agility and modernisation, with weighted-mean scores of 1.54 and 1.45, respectively, are considered very pertinent by 54% and 61%, respectively, of the responding IBs, as shown in Figure 2.2. Digitalisation is also considered pertinent for strengthening core competencies, and enhancing both operational efficiency and revenue generation, with weighted-mean scores of 1.57, 1.4 and 1.57, respectively, as shown in Figure 2.1. This is corroborated by 51%, 67%, and 45%, respectively, among responding IBs that indicated they "strongly agree", as per Figure 2.2.

2.3 COVID-19 and digital transformation in IBs

The need to ensure physical distancing due to COVID-19 recorded a weighted-mean score of 1.24, as shown in Figure 2.1. Arguably, the outbreak of COVID-19 and the consequential need for physical distancing and efficient disbursement of funds to the needy have amplified the indispensability of digitalisation of banking services. Figure 2.2 indicates that 69% of the respondent IBs "strongly agree" that the pandemic is an important reason for their digitalisation process. Although cutting across all jurisdictions, most of the responses were from IBs from Bangladesh, Indonesia, Nigeria and Pakistan.

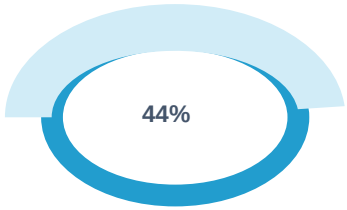
As a strategy to reduce the infection rate, contactless digital payments between persons as well as for purchases in stores have been greatly encouraged since the outbreak of the pandemic. Incentives to use digital payments have also been provided in some instances, especially in developing countries.[36] The increased experience with online banking due to the restrictions on movement, especially since the first wave of the pandemic, does not favour the physical service delivery that bank branches are meant to provide.

As shown in figure 2.3, prior to the COVID-19 pandemic, 44% of the responding IBs did not implement the work-from-home (WFH) policy. The pandemic has necessitated that 34% of the IBs implement a rotational WFH/ work-from-office (WFO) policy with staff coming to the office on alternate days of the week. About 20% of the responding IBs indicate that they have implemented a blend of 25% WFH; 75% WFO, or 25% WFO; 75% WFH policy depending on the stringency and duration of the lockdown in their respective jurisdictions. IBs need to get used to this new normal of staff working from home by enhancing their teleworking and remote access capabilities without compromising on the integrity of their technology network.

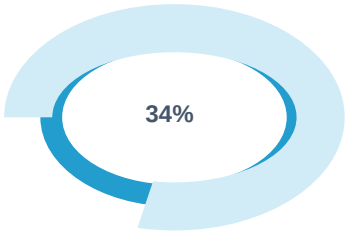
In response to how effective the WFH policy has been, 42% of the respondent IBs stated that the nature of banking operations would require that some technical and administrative matters can only be conducted at the office. Although 19% stated that with the requisite supporting digital infrastructure, WFH can be applied for most types of activities, 32% noted that adopting WFH makes them more susceptible to cyber risk.

[36] I. Agur, M.S. Peria and C. Rochon (2020), *Digital Financial Services and the Pandemic: Opportunities and Risks for Emerging and Developing Economies*, International Monetary Fund Special Series on COVID-19: https://www.imf.org/~/media/Files/Publications/covid19-special-notes/en-special-series-on-covid-19-digital-financial-services-and-the-pandemic.ashx

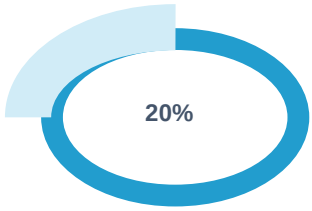
Figure 2.3. Work from Home Policy in IBs due to COVID-19



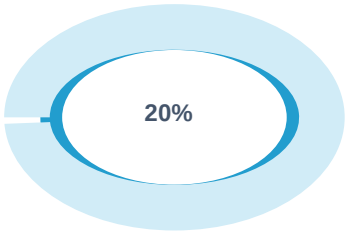
IBs that did not implement WFH policy pre-COVID-19



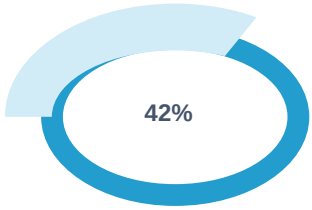
IBs that implement rotational WFH policy since COVID-19 outbreak



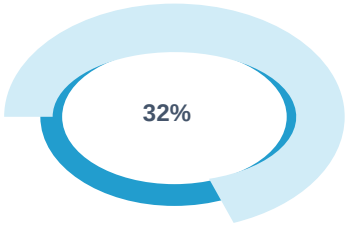
IBs operating 25% WFH and 75%WFO policy



IBs operating 25% WFO and 75% WFH policy



IBs that consider that some technical and administrative matters cannot be conducted from home office.



IBs that consider WFH policy makes them prone to cyber risk

Source: IFSB Survey, 2020.

2.4 Status of Islamic Banking Digitalisation

Three questions addressed the respondents' current state of digital transformation. These relate specifically to the proportion of their digital operation, as well as to the proportion of their most recent budget spent on the digital transformation process.

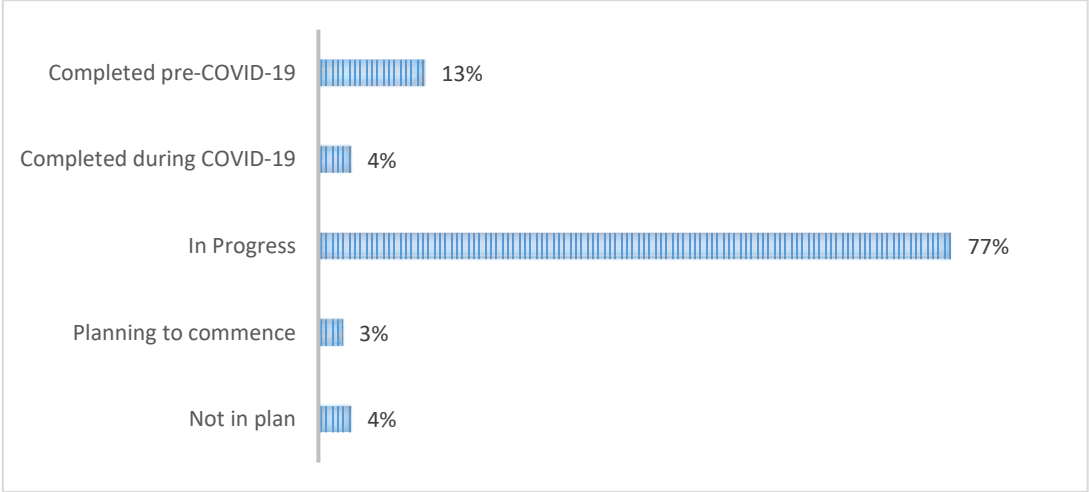
As shown in Figure 2.4, most IBs (77%) cutting across all jurisdictions indicate that their digital transformation process is in progress. Although the specific status is unknown, the fact that a process is under way is promising. This is because the swift changes in technological advancement imply that the proliferation of disruptive financial technology and the rate of adoption by IBs will not only be unprecedented but is also unlikely to abate any time soon.

Only 3% are planning to commence related digital transformation activities; while another 4% have no related plan at the moment.[37] Of the remaining IBs, 13% indicate that they had already

[37] These respondent IBs are from the UAE.

completed the necessary processes prior to the outbreak of COVID-19. These IBs are from Bahrain, Kuwait, Malaysia, Singapore, and UAE. Only 4% of the respondent IBs[38] completed their digital transformation process during the pandemic.

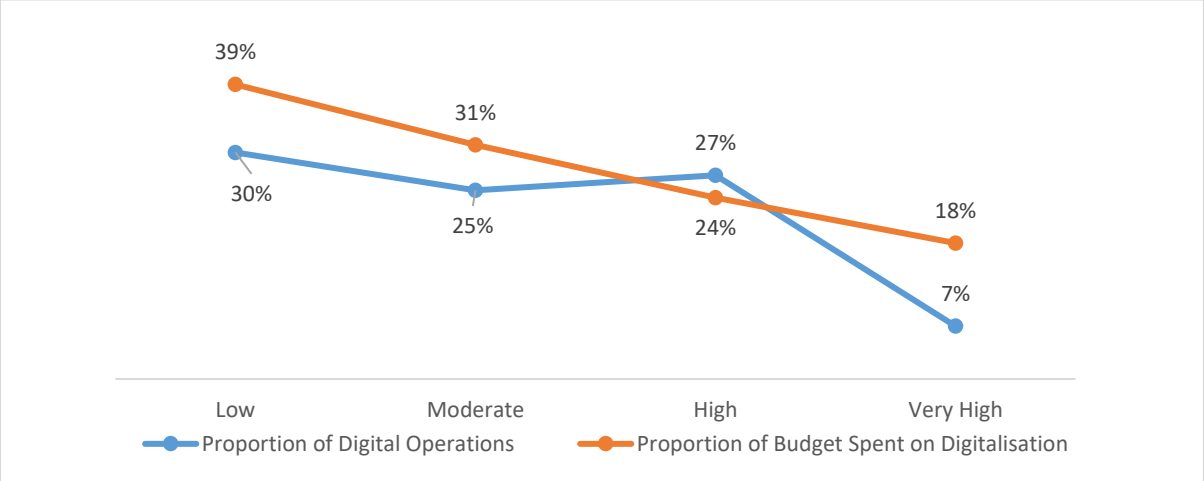
Figure 2.4 Status of IBs Implementation of Digital Transformation



Source: IFSB Survey, 2020

Figure 2.5 divides the proportion of the digital operation of the IBs, as well as the proportion of the most recent IT budget spent on digital transformation activities, into four categories[39]. As indicated in the Figure, while 30% of the IBs indicate that their digital operations are at a low level, 39% also indicate that they spent a low proportion of their most recent IT budgets on digital transformation. Except in few instances of some IBs from Bahrain, Brunei, Pakistan, Jordan, Saudi Arabia, and UAE, most are from non-systemically important Islamic banking jurisdictions.

Figure 2.5 Proportion of IBs Digital Operation and Most Recent IT Budget Spent



Source: IFSB Survey, 2020

For the 25% of the IBs that consider the proportion of digital operations to be moderate, a corresponding moderate proportion of IT budget spent on digitalisation is indicated by 31%. In

[38] These are from both Bangladesh and Pakistan.
[39] Low = up to 25%, Moderate = 25% -50%, High = 51% - 75%, Very High = 76% - 100%.

both low and moderate classifications, the proportion of digital activities is lower than the proportion of IT budget spent among the respondent IBs. This is perhaps an indication that notwithstanding these IBs' current relatively lower level of digital operations, they are committing a higher proportion of funds to digitalisation. Capital spending on digitalisation is higher at the initial stage given there is a minimum scale that needs to be attained. Nonetheless, if the momentum is maintained, scaling up digital operations will be less cumbersome for these IBs as digitalisation becomes inevitable due to the numerous benefits it offers.

Furthermore, while 27% of the IBs indicate that a high proportion of their operations is digitalised, 24% indicate that they also spent a high proportion of their most recent IT budgets on digital transformation. In the fourth category, 7% of the IBs indicate that a very high proportion of their operations is digitalised, while 18% of their IT budget is spent on digital transformation. Some of the respondent IBs in this fourth category indicate that huge sums of money have been spent over the years on an outright overhaul of legacy infrastructures for information sharing among stakeholders, as well as to strengthen cyber-security units with the requisite human talents, especially domain specialists. Most of these IBs have also completed their digitalisation process prior to the outbreak of COVID-19. Perhaps, the relatively lower proportion of recent IT budget spent on digitalisation is a reflection of the high level of proficiency and other benefits that accrue from previous periods' related IT spending.

In another part of the survey, 8% of IBs indicate that their spending on digital transformation will remain unchanged from their pre-COVID-19 level. A cross-tabulation analysis also indicates that this group is part of those IBs that spent a very high proportion of their IT budget on digital transformation.

The other 92% of the respondent IBs indicate that the proportion of their spending on digital transformation will likely increase due to the COVID-19 pandemic. For this group, a Chi-square test of independence was performed to examine the relation between the proportion of digital activities and proportion of IT budget spent on digital transformation. The relation between both variables is positive and significant, X^2 (1, N = 56) = 28.31, p = .0008. A Cramer's V. of 0.41 also indicates a strong effect between the two variables implying that as digital activities are scaled-up, the proportion of the IT budget spent will also be scaled-up.

SECTION 3: TECHNOLOGY AND PRUDENTIAL RISKS IN IBs' DIGITALISATION

3.1 Technological Advances Adopted in Digital Transfromation of IBs

Responses to the question on the various technological advances being adopted by the IBs indicate that related digital banking activities are already taking place in the Islamic banking industry. As indicated in Figure 3.1, the three most adopted technologies are mobile and digital wallets (93%), application programming interfaces (91%) and biometric authentication (87%). The three least used technologies are robo-advisory (27%), distributed ledger technology (DLT) and smart contract (26%), and Internet of Things (23%).

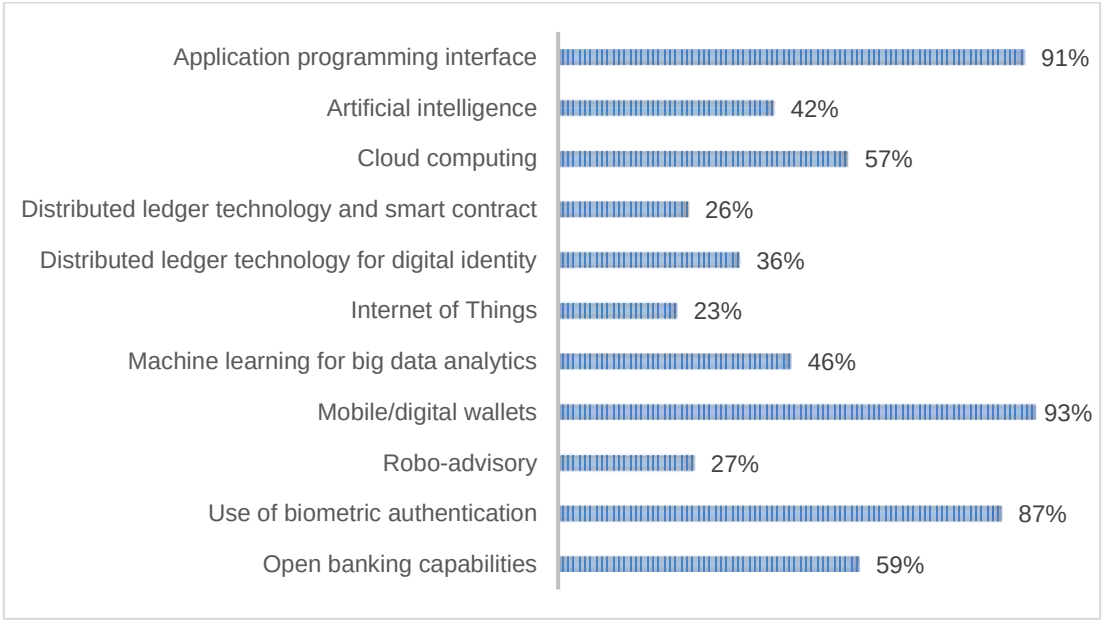
Numerous IBs have introduced various mobile banking apps and digital wallets,[40] which are among the most popularly deployed technologies – especially for deliveries and e-hailing services. Their usefulness especially for financial inclusion through payment services and

[40] The digital wallet gives users access to money stored in a digital form, enabling them to make payments to connected payment terminals regardless of whether or not the holder has a bank account.

financing is well noted in jurisdictions with a low penetration of bank account ownership but a high rate of access to mobile smartphones, especially among millennials.[41]

In addition, "cardless cash withdrawal" has also been recently introduced in Islamic banking as a mobile banking app. With this, customers can use their mobile smartphone number to transfer funds to an intended recipient who may not necessarily have a bank account. The recipient receives an SMS with a one-time personal identification number (PIN) that can be used to withdraw cash from the closest automated teller machine (ATM) of the IB without a debit or credit card.

Figure 3.1 Technological Advances Adopted by IBs



Source: IFSB Survey, 2020.

Mobile wallets are also very useful for flattening the curve of the spread of COVID-19 by allowing users to make contactless payments based on a near field communication (NFC) technology in which case a mobile device is held within a short distance from a point-of-sale (POS) terminal.[42] This offers a lot of benefits to users including convenience of not needing to carry physical cards or remembering PINs. Some IBs also introduced Chat Banking via the WhatsApp platform. This is to further enhance the experience and engagement of the patrons of their digital banking channels who will be able to perform a myriad of financial transactions in a secure and confidential manner over the platform.[43]

The widespread adoption of API among the respondent IBs also reflects the increased use of APIs within the global financial ecosystem, up from 1 in 2005 to 17,000 in 2017.[44] API connects software programs and allows them to communicate based on programming code,[45] bringing about efficient and reliable interactions among computerised systems. APIs allow for secured

[41] Conversely, a new form of exclusion could also be created, especially among the elderly or extremely poor people who do not have access to mobile technology or smartphones.
[42] Other notable technologies used to render mobile wallets services include magnetic secure transmission (MST), Quick Response (QR) codes, Bluetooth, and short message services (SMS).
[43] https://www.zawya.com/mena/en/press-releases/story/Emirates_Islamic_becomes_worlds_first_Islamic_bank_to_launch_banking_via_WhatsApp-ZAWYA20190407092519/
[44] FSB (2019), *FinTech and Market Structure in Financial Services: Market Developments and Potential Financial Stability Implications*: https://www.fsb.org/wp-content/uploads/P140219.pdf
[45] *State of the Global Islamic Economy Report, 2018/2019*, p. 18: https://haladinar.io/hdn/doc/report2018.pdf

data sharing and analytics among disparate systems and separate financial institutions, especially in open banking applications.[46] Nonetheless, when not properly secured, the adoption of APIs can lead to market structure fragility and may trigger network instability, with contagion effects, in the event of a breakdown. APIs may also influence customer switching behaviour with their significant impact on deposits as a source of funding for financial institutions.[47]

The widespread use of biometric authentication by IBs, as indicated by the responses provided to the survey, could be due to its streamlining of authentication processes. Other security benefits are provided through the use of stable and unique biometric features for recognition – for instance, fingerprints, voice, face, iris patterns or some other internal features. Some jurisdictions also use a biometric verification number that is unique to every bank customer regardless of the number of accounts operated with the same or different banks within a jurisdiction. The use of this technology extends beyond biometric identification that answers the question of "Who are you?", because authentication requires proof of who the user is prior to their gaining access to a desired financial service.

Biometric authentication via smartphones with pre-installed fingerprint scanners has increased the use of this technology. Typically, it is used for limited services such as checking account balances or transferring a limited amount between pre-registered and verified accounts via a mobile banking application. This technology is less susceptible to theft, spoofing and online phishing, which are quite common with password authentication.

In a scenario like that of the current COVID-19 pandemic, this technology could also help with remote customer on-boarding without infringing on the customer due diligence process. This may result not only in increased market penetration, as indicated by 59% of the IBs as per Figure 2.2, but also in reduced operating costs of call centres for password resets, for instance.

Cloud computing has also been very much deployed, especially for unbundling of services as well as for data sharing in open banking applications. More than half (57%) of the respondent IBs indicate that they adopt cloud technology. This perhaps reflects a gradual shift among IBs from an on-premises data service to a public cloud-based data service.

The possibility of technology externalisation due to the proliferation of technology vendors and platforms that offer cloud services would significantly reduce IBs' infrastructure and human resource requirements costs. However, IBs may have to contend with providing financial services on platforms they neither own nor have control over. This could have implications for financial stability in the event of a breach or cyber-attack on the part of the cloud service provider.

The use of software applications, especially for payments and transaction services is becoming fundamental to IBs' operations due to increasing contestability and competition. Robotics process automation, machine learning and AI technology are now pervasive. IBs are expected to use these technologies more for repeatable transactional tasks, as well as predictive analytics based on big data, cloud computing and the IoT to better anticipate customer needs. For instance, an IB, as part of its innovation and digital transformation

[46] According to the FSB (2019), "open banking operations" refers to a system in which financial institutions' data can be shared for users and third-party developers through APIs: *FinTech and Market Structure in Financial Services: Market Developments and Potential Financial Stability Implications*

[47] The World Bank Group (2019), "Prudential Regulatory and Supervisory Practices for FinTech: Payments, Credit and Deposits": http://documents1.worldbank.org/curated/en/954851578602363164/pdf/Prudential-Regulatory-and-Supervisory-Practices-for-Fintech-Payments-Credit-and-Deposits.pdf

process to enhance customer experience and convenience, unveiled its digital virtual employee which will digitally provide FinTech tips and insights as well as information on the Islamic bank's products and services.[48]

Based on the alignment of its operational principles with Sharī'ah principles such as trust, transparency, traceability, fairness and equality, IBs have also applied blockchain technology in their various operations. Specifically, 36% of the respondent IBs, as shown in Figure 3.1, indicate that they apply this technology. When combined with AI and complemented with cloud computing, IBs' operational resilience and regulatory compliance can be enhanced through facilitation of customer due diligence and prevention of fraud and irregularities. Although still at a very early stage, blockchain technology in Islamic finance is mainly in cryptocurrency,[49] which has attracted a variety of rulings among Sharī'ah scholars but seems to be gaining traction.[50] Some FinTech firms have obtained certification for the Sharī'ah compliance of their digital currencies in their respective jurisdictions.[51]

As indicated by 26% of the respondent IBs, blockchain technology is also increasingly being used for the operation of smart contracts in Islamic banking. In this case, programmable applications have been employed to self-verify and self-execute Sharī'ah-compliant financial transactions. For instance, while appearing virtually to all network users, automatic change of ownership or adjustment to financial flow in a contractual transaction can be triggered due to the occurrence of specified events in the contractual clause.[52] Some IBs have also used blockchain in their cheque-based payment process, as well as for *ṣukūk* issuance, to authenticate transactions and mitigate the potential for fraud.

With the support of multilateral organisations such as the Islamic Corporation for the Development of the Private Sector (ICD), further options are still being explored by start-ups to deploy blockchain technology for Sharī'ah-compliant liquidity management, interbank relations and commodity transactions. Other areas being explored include using smart contracts based on blockchain technology to automate the entire contractual process of institutions offering Islamic financial services.[53]

3.2 Types of Technology in which IBs are Currently Investing

In addition, the IBs were asked to indicate which among the listed variants of technology they are presently investing in as part of their digital transformation process. As shown in Figure 3.2, the distribution also reflects that observed earlier in Figure 3.1. Most IBs (specifically, 82%) are currently investing in mobile application technology, while 68% are investing in biometric authentication techniques, as per Figure 3.2.

Regarding other technologies, 60% of the IBs are currently investing in security and privacy technologies, while 59% are also investing in NFC, QR codes and SMS technology. Furthermore, 59% indicate a current expenditure on business intelligence, data and analytics.

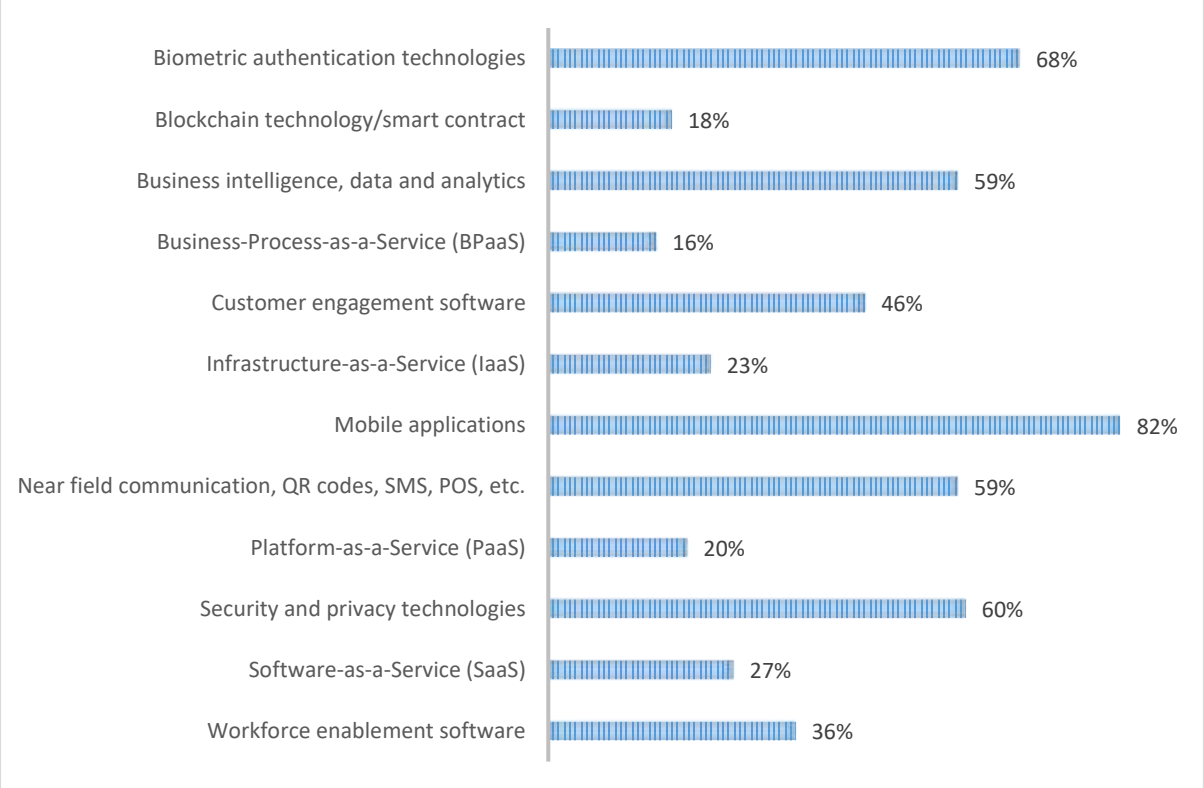
---

[48] https://wanbabablog.com/2019/05/28/bahrain-islamic-bank-unveils-its-first-virtual-employee/
[49] N. Alam, L. Gupta and A. Zameni (2019), *Fintech and Islamic Finance*. Switzerland: Palgrave Macmillan.
[50] Mufti Muhammad Abu-Bakar (2019), *Sharī'ah Analysis of Bitcoin, Cryptocurrency, and Blockchain*: https://blossomfinance.com/bitcoin-working-paper
[51] Some examples include HelloGold in Malaysia, which received certification from Amanie Advisors, and Blossom Finance in Indonesia. There is also Qintar, a Switzerland-based firm that launched its first Sharī'ah-compliant coin. Similarly, Switzerland-based X8 AG and Bahrain-based Rain have also obtained certification from the Sharī'ah Review Bureau in Bahrain. Adab Solutions, based in the UAE also launched its First Islamic Crypto Exchange (FICE), which has since passed legal registration in Bahrain.
[52] N.R. Mohd. Zain, E.R. Engku Ali, A. Adewale and H. Abdul Rahman (2019), "Smart Contracts in Blockchain: An Exploration of the Legal Framework in Malaysia", *Intellectual Discourse*, 27(2).
[53] https://ifikr.isra.my/news/post/blockchain-is-making-its-way-into-islamic-finance

This reflects the fact that even though customer convenience, preference and experience are being prioritised, it is not at the expense of data and privacy protection. Only 15% of IBs are currently investing in smart contracts via blockchain technology.

The cloud computing service model receiving most investment is Software-as-a-Service (SaaS), as indicated by 27% of the respondent IBs. This perhaps is due to its relatively lower costs, reduced time to benefit, scalability and integration, ease of use, and upgrades possibility.[54] Infrastructure-as-a-Service (IaaS), which is considered the most relevant level of cloud service to financial institutions for processing core banking systems and storing critical data in the cloud,[55] is being invested in by 21% of the responding IBs. IaaS allows users to access cloud services on a pay-as-you-go basis. Apparently in response to the new normal of staff working from home due to COVID-19, 34% of the responding IBs indicate they are also expending on requisite workforce enablement software to enhance their teleworking and remote access capabilities.

Figure 3.2 Current Expenditure on Technological Advancements by IBs.



Source: IFSB Survey, 2020.

In terms of which aspects of the IBs' digital transformation is most costly, 44% of respondents indicated their highest expenditure is on providing and investing in online platforms and security systems, 35% indicated digital banking infrastructure, and 11% indicated maintaining their existing digital system. Staff training is considered the least costly aspect of digital transformation by 11% of the IBs. This distribution also reflects the response of the IBs to

[54] https://www.ibm.com/cloud/blog/top-5-advantages-of-software-as-a-service
[55] The World Bank Group (2019), "Prudential Regulatory and Supervisory Practices for FinTech: Payments, Credit and Deposits", p. 5: http://documents1.worldbank.org/curated/en/954851578602363164/pdf/Prudential-Regulatory-and-Supervisory-Practices-for-Fintech-Payments-Credit-and-Deposits.pdf

questions relating to the challenges to implementing digitalisation, with legacy infrastructure and lack of requisite human capital considered among the top issues.

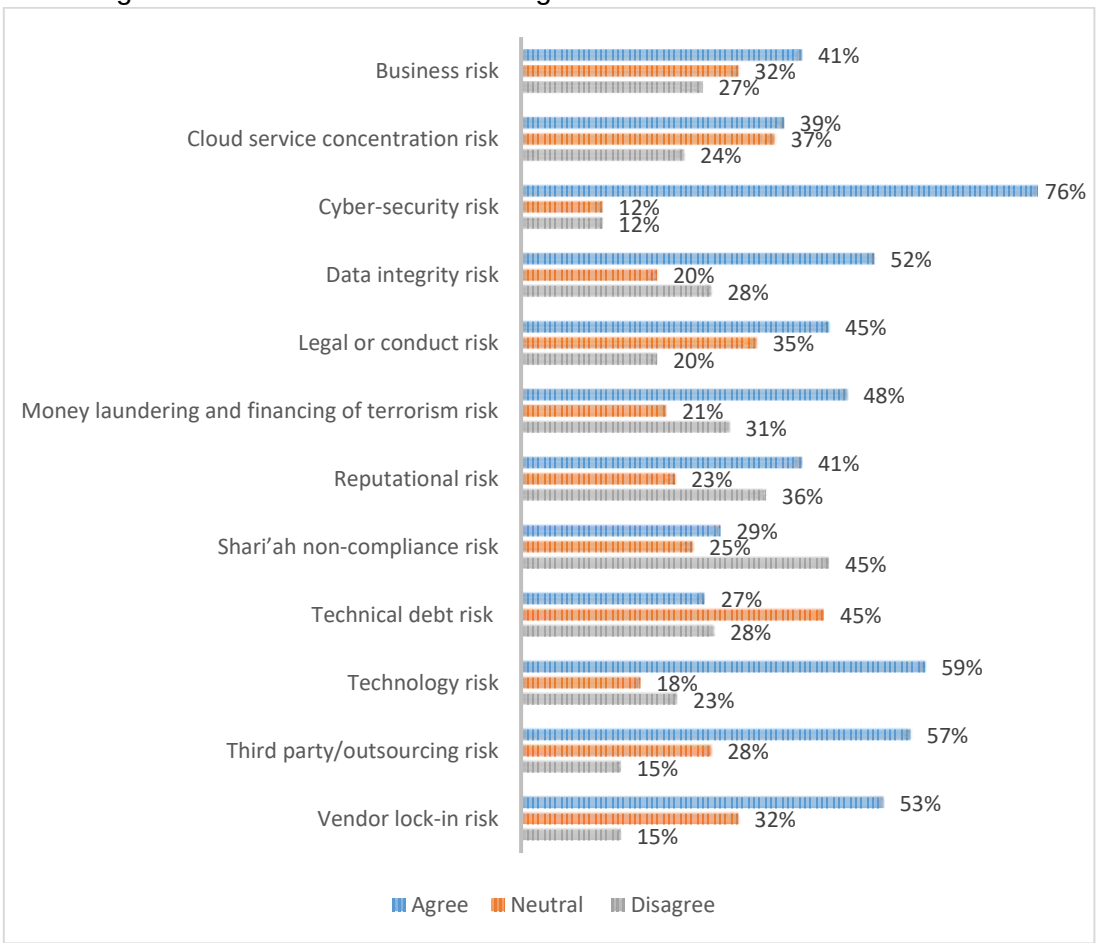
In terms of what the IBs consider will account for their highest expenditure on digitalisation in the near future, 53% stated the costs of mitigating cyber risk and related digital risks. The cost of upgrading their existing system is indicated by 21%, while 18% nominated ensuring the operational efficiency of their digital system. This distribution, which reflects the IBs' consideration of cyber security as their main prudential risk, also implies a low level of exposure to technical debt risk.

The remaining 8% of respondents indicate that most of their future expenditure on digitalisation would relate to collaboration and cooperation with digital start-ups. Perhaps, most IBs are likely to be exploring the possibility of ownership via a partial or total buy-out, or sponsorship with the new entrants, in an attempt to avoid switching costs, and to tap into the huge opportunities to earn income from interchange fees to be paid by the start-ups.

3.3 Prudential Risks Faced by IBs in their Digitalisation Process

Technological adoption has not only opened the way to new possibilities and enhanced the operational efficiency of IBs, but has also created potential risks. Responses obtained from the IBs that participated in the survey indicate that risks relating to cyber security, technology, third-party/outsourcing, and data integrity are of concern. The distribution of responses provided by the IBs is shown in Figure 3.3.

Figure 3.3 Digital Transformation Risks Facing IBs



Source: IFSB Survey, 2020

Cyber-security risk seems to be the main prudential risk facing the IBs in their digital operation especially those from Bahrain, Brunei, Egypt, Kuwait, Qatar, Saudi Arabia, and UAE. This risk is indicated by 76% of the IBs. The swift changes in technological advancement make the legacy infrastructure of many IBs highly susceptible to cyber risk. In fact, the CIBAFI Islamic Global Bankers' Survey in 2019 ranked cyber risk as the number one risk facing IBs.

This may not necessarily be an issue peculiar to IBs, as conventional banks are also faced with the issue of cyber security. As such, the potential for the occurrence of a cyber-attack on any financial institution is more a matter of *whe*n than *if*. It is projected that the cost of global cybercrime will reach USD 6 trillion by 2021.[56] The effects of such attacks on perceptions about data integrity – indicated by 52% of the responding IBs – may also significantly interrupt business operations and have implications for public confidence in the technology.

High susceptibility to cyber-security risk may also create reputational risk for an IB's digital operation, as highlighted by 41% of the respondents. Given the implications of cyber-risk occurrence for financial stability, the focus of IBs should therefore transcend cyber-risk prevention. Such a focus should also cover response, recovery and adaptation, given that cyber risks are difficult to pre-empt yet evolve and transform swiftly with no trace of perpetrators.

The FSB already notes the financial stability implications of such, especially in the event of a cyber-attack on or an operational failure of cloud services. In a case where quite a number of IBs rely on a few dominant cloud service suppliers, this could pose a systemic risk triggered by "cloud concentration" risk due to operational centrality of computing services.[57] This risk is also indicated by 39% of the respondent IBs. The effects of such failures on perceptions of data integrity could also have implications for public confidence in the technology, thus creating reputational risk.

Other related prudential risks are legal risks and data security risks, indicated by 42% and 50% of the IBs, respectively. The former could arise due to the fragmented payment market, where the large number of innovative products and services makes governance, management and control rather complex. For instance, in the use of biometric authentication technology, a false acceptance or false rejection could arise, depending on the unique biometric feature used. This could have implications for users' experience, thus leading to legal or reputational risks for an IB.

In terms of data security risk, the manifestation depends on the type of technology deployed. There could be issues arising from dependency on, for instance, mobile device manufacturers or third-party wallets. The proliferation of viruses and malwares, as well as the danger of lost or stolen mobile devices, could also heighten the risk of unauthorised payments.[58]

Reliance on third-party smartphone manufacturers and the pre-installed biometric authentication technology in the devices also means financial institutions have no direct control of a technology that is crucial to their operational efficiency. This exposes them to third-party risk, which is indicated by 59% of the responding IBs. In addition to the fact that, unlike a password, a fingerprint cannot be changed if accessed without consent, a potential data

[56] https://www.insurancebusinessmag.com/ca/news/cyber/the-key-cyber-trends-keeping-insurance-professionals-up-at-night-171709.aspx

[57] R. Harmon (2018), "Cloud Concentration Risk: Will This be our Next Systemic Risk Event?", Cloudera White Paper: https://www.researchgate.net/publication/331099204_Cloud_Concentration_Risk_Will_this_be_our_next_Systemic_Risk_event

[58] http://www.fundacionmicrofinanzasbbva.org/revistaprogreso/wp-content/uploads/2018/08/pub-ReportonprudentialrisksandopportunitiesarisingforinstitutionsfromFinTech.pdf

security risk could result from residual attacks due to the possibility of collecting fingerprints from various objects touched by a customer or even fingerprint sensors.

Vendor lock-in risk is indicated by 53% of the responding IBs as having prudential implications arising from digitalisation of their banking operations. This risk would arise where an IB is dependent on a particular service provider – for instance, for cloud services – and cannot switch to a different vendor without incurring significant costs, facing legal action or suffering technical incompatibilities. This raises concerns for movement of data in and out of the cloud, data ownership and confidentiality, and susceptibility to cyber breaches, with implications for business operations. The susceptibility of an IB to this risk would depend on the extent to which it retains flexibility to switch to other providers as and when the need arises.[59]

Although 59% of the respondent IBs strongly agree that technology risks have prudential implications for the digitalisation of their banking operations, only 29% indicate that technical debt is a concern. The former risk occurs where either unsuitable or outdated technology is deployed for the daily operations of the bank, such as reconciliation of books of accounts. The latter occurs where avoidable additional costs would have to be incurred later by adopting and investing in a cheaper technology now as a short-term fix at the expense of a more expensive, efficient and effective alternative.

As indicated in Figure 3.3, almost half (48%) of the respondent IBs indicate they strongly agree that money laundering (ML) and financing terrorism (FT) risk might have prudential implications arising from digitalising their operations. This concern is not peculiar to IBs, given that the perpetration of such crimes is driven more by opportunity and convenience than by an institution or transaction following Islamic banking. Nonetheless, the proliferation of innovative financial products and processes due to financial technology should not make IBs more susceptible to ML/FT activities in such a way that money launderers might use the sophisticated methods employed by financial institutions to launder illicit funds.[60]

From a prudential risk perspective, Sharīʿah non-compliance risk could crystallise from the use of mobile wallets, for instance. This could also potentially impact on the risk profile of an IB, as indicated by 29% of the survey respondents. Such a risk could result from concerns that border on the non-specificity of the contracts upon which such mobile wallets are offered, as well as the modus operandi involved.

Related questions include but not limited to: are funds in these wallets based on *qarḍ* or *wadīʿah*? Are the promised rewards, which are based on luck in some instances and are guaranteed in others, a form of *hibah* or returns? Can this be applicable if the funds placed in the wallets are based on *qarḍ*? Can the funds be based on equity-based contracts such as *muḍārabah* and *mushārakah* given that the deposits are guaranteed? Prior to being used by depositors, are the wallet funds used for *Sharīʿah*-compliant purposes by the digital wallet providers? These and related questions raise concerns about the need for Sharīʿah considerations in digital products and financial apps development in response to the perceived "Sharīʿah neutrality" of technology and financial apps.[61]

[59] J. Opara-Martins, R. Sahandi and F. Tian (2016), "Critical Analysis of Vendor Lock-ins and its <Pls check title> Impact on Cloud Computing Migration: A Business Perspective", *Journal of Cloud Computing: Advances, Systems and Applications*, 5(4).
[60] M.S. Al Mamun, A.A. Adewale, G. Abu Mwis and N. Youssef (2019), *Money Laundering and Financing of Terrorism (ML/FT) Risks in Islamic Banking*, IFSB Working Paper Series WP-12/12/2019: https://www.ifsb.org/download.php?id=5509&lang=English&pg=/sec03.php
[61] https://islamicbankers.me/2019/01/15/e-wallets-did-you-forget-us-again/

Additional remarks provided by some of the respondent IBs indicate that Sharīʿah non-compliance risk could also occur indirectly due to a breach of Sharīʿah requirements, the order or number of critical steps involved in a contract, etc. For instance, in a commodity *murābaḥah* for Islamic personal financing, an IB purchases a commodity from a broker and sells it on deferred payment basis to the customer requesting personal financing. The IB, acting as an agent for a fee on behalf of the customer can only disburse personal financing to such customer from cash generated from selling that commodity to a different commodity broker. While digitalisation can help improve and quicken the hitherto manual processes, omission or wrong sequencing of any of the steps involved renders the transaction Sharīʿah non-compliant.

Systems control could also malfunction in the event of a system error or bugs compromising Sharīʿah requirement parameters. One respondent IB cited an instance where, due to tagging error, a system omits the *"Aqd"*[62] renewal, thus allowing financing of non-Sharīʿah compliant shares. Another instance is error in computation method of profit/charges, or in the selling price capping mechanism that could cause a profit overcharge.

Another issue often mentioned is that of *khiyar* (option) in the application of smart contract. For instance, in a smart-contract based *muḍārabah* transaction, due to automation of the processes involved neither the *muḍārib* nor the *rabb al- māl* can terminate the contract. Whereas, contractually either have the right to do so except when the former has commenced work or where the contract is for a specified time which has not lapsed. In order to leverage on the benefits of the smart contract but also prevent Sharīʿah -non-compliance risk, explicit mention and prior agreement would have to be made between contracting parties that regardless, the *muḍārabah* contract cannot be modified nor terminated prior to completion.

Conversely, some respondents stated that such Sharīʿah non-compliance may not necessarily occur in their digitalisation activities. This is because technology is viewed only as a platform through which Sharīʿah-compliant products are offered. All existing and new initiatives in their IB's operation would have to go through the Sharīʿah Compliance Unit, the Advisory Council of Experts (ACE) or the Sharīʿah board, as provided in their respective jurisdictions. This provision mitigates against such Sharīʿah non-compliance risk in digital Islamic banking.

Business risk is indicated by 41% of the respondent IBs as a likely consequence of digitalising their banking operations. IBs face stiff competition from FinTechs and BigTechs, and the increased possibility of new disruptors entering the market, thus heightening competition and contestability. These competitors operate under a lower cost structure and lesser strict regulation. In contrast, the substantial investments required by IBs to upgrade or replace legacy technology infrastructures would weaken their financial position in the short-term especially during downswings in the economy as being presently witnessed due to the COVID-19 pandemic.

Furthermore, the reduced costs and efforts required by customers for shopping around and switching banks due to technology may erode IBs' brand advantage and make customers less sticky. This will also have implications for the stickiness of deposits and investment accounts as cheap and stable sources of funding to IBs. This is because customers will be able to easily and frequently optimise their surplus balances by moving funds from a lowly-remunerated transaction accounts to a more productive and higher rate of return paying accounts or investments.

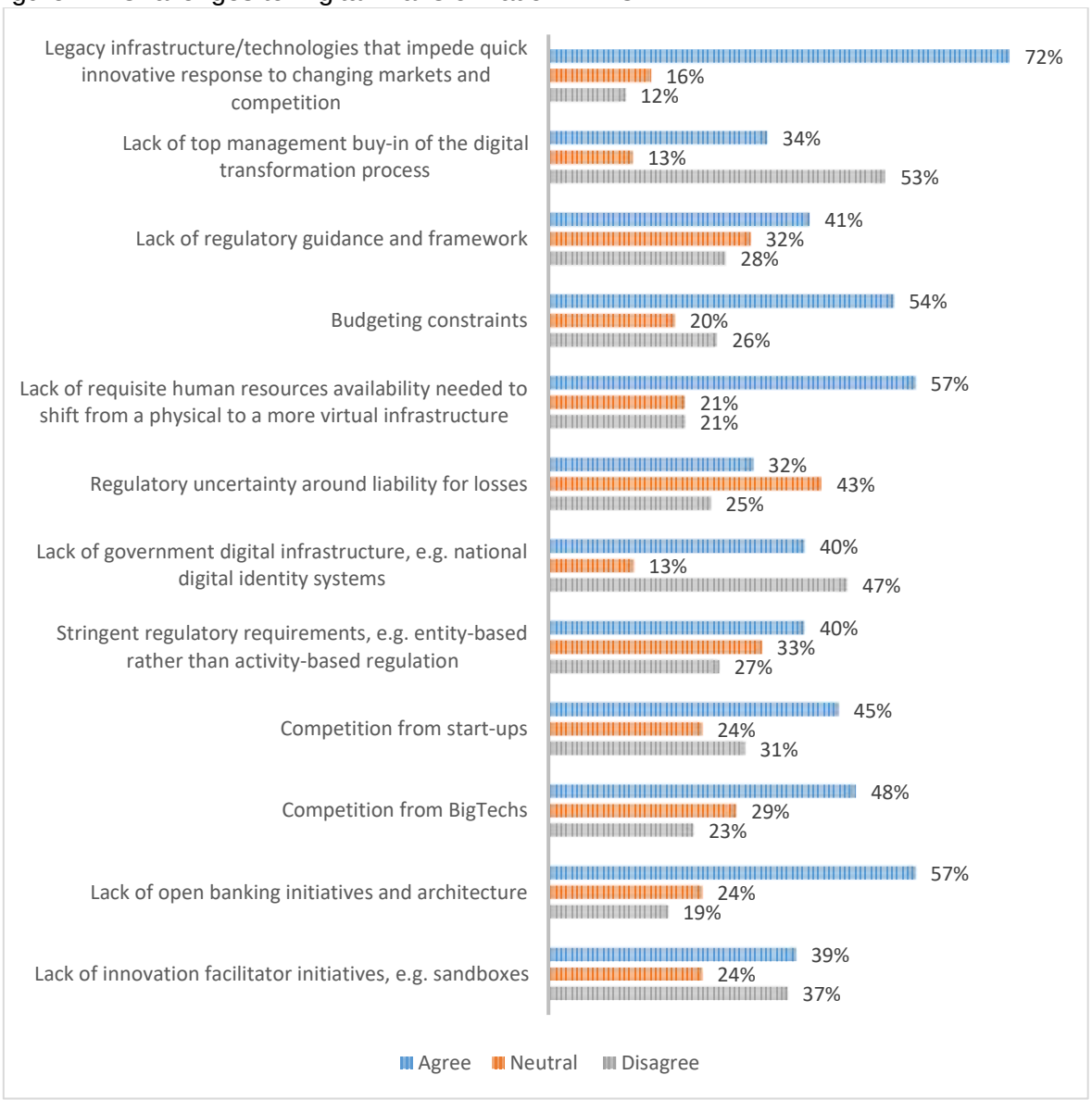
[62] An agreement between two willing parties to initiate, adjust or terminate a given transaction in a manner binding upon both parties.

SECTION 4: CHALLENGES AND REGULATORY APPROACH TO IBs' DIGITALISATION

4.1 Challenges to Digital Transformation in IBs

IBs were also asked about factors that impede their digital transformation process. A list of such factors drawn from various publications was provided, with response options indicating level of agreement or otherwise on a scale ranging from "strongly agree" to "strongly disagree". Responses obtained as shown in Figure 4.1 indicate that the most pressing factors relate to legacy infrastructure, lack of open banking initiatives, budgeting constraints and lack of requisite human capital. Issues relating to regulatory uncertainty and lack of top management support are among the least-cited impediments to the digital transformation process in IBs.

Figure 4.1 Challenges to Digital Transformation in IBs



Source: IFSB Survey, 2020.

Based on the responses obtained, 74% of the IBs indicated that legacy infrastructure and technologies impede their response to changing market dynamics and competition driven by technology. Perhaps there are concerns for IBs relating to mitigating operational risks that

may crystallise from using legacy technology infrastructure to cope with the rate and speed of technological transformation today. There will be even more pressure where the IBs still rely on obsolete legacy infrastructure, outdated applications, siloed data platforms, an overextended branch network, disparate data sources, and rigid internal operations and culture. Not only would these hinder the IBs' usage of the huge amount of data at their disposal, but it also makes them highly susceptible to, for instance, cyber risks.

As shown in Figure 4.1, 57% of the IBs especially those from Bahrain, Brunei, Indonesia and Sudan strongly agree that lack of the requisite human capital needed for digitalised banking such as data analysts may be an impediment. Human capital development is a fundamentally important pillar for innovation to be successful. The digital transformation process requires highly specialised human capital and domain experts. For instance, as automation of most banking operations becomes the new norm, a new competency model would also become pertinent in the human capital strategy of the IBs.

Providers of digital Islamic financial services will therefore need to retrain and reskill existing talent even as they make efforts to attract new talent that fits the imminent digital workforce transformation of the banking workforce. This process may not be as straight-forward as presented, for a number of reasons. For instance, attracting and recruiting the right talent may involve looking beyond the financial services industry, or even beyond a particular jurisdiction. In addition, most of these potential talents are likely to be millennials, whose expectations and preferences regarding remuneration, work flexibility in terms of location and time, as well as opportunities for development would suit competitors such as FinTechs and BigTechs better than the IBs.

Budgeting constraints are also indicated as an impediment to digitalising Islamic banking operations by 57% of the respondent IBs, mainly those from Indonesia, Jordan, Sudan. The need to replace legacy infrastructures to enhance their competitiveness during and post-COVID-19 will further strengthen the effects of budgeting constraints on implementing digital transformation. As shown in Figure 4.1, 70% of the responding IBs spent less than 50% of their most recent budget on IT, and 45% indicated that more than 50% of their operation is digitalised. This may imply that IBs have hitherto not been spending much on technology, but may have to do so now for the reasons stated earlier. However, while this may yield a favourable outcome in the future, as IBs leverage on technology, it will put immediate pressure on their capital expenditure.

The lack of open banking initiatives and architecture is indicated by 57% of the responding IBs, while 39% cited the lack of innovation facilitator initiatives such as regulatory sandboxes. Although quite a number of the jurisdictions where Islamic banking is operated have provided such requisite infrastructure and initiatives, there are still challenges. For instance, there are concerns regarding the performance and interoperability of banks' APIs due to lack of compatibility with legacy infrastructures, lack of standardisation, security risks etc. Also, regulatory sandboxes still need to thoroughly assess the relevance and benefits of their solutions to the domestic Islamic banking market.

Similarly, IBs' resistance due to infrastructure setbacks and the lack of technical standards could also have impeded implementation of open banking in some jurisdictions. Such regulatory uncertainty and lack of regulatory guidance are indicated by 32% and 34% of the respondent IBs, respectively.

Competition from both FinTechs and BigTechs was indicated by 45% and 48%, respectively, of the respondent IBs as a digitalisation challenge they are having to confront. IBs from jurisdictions where IBs are systemically important generally consider competition from the BigTechs as more of a challenge compared to IBs from jurisdictions where Islamic banking is non-systemically important.

The effect of the BigTechs in this instance will be clearer, especially when they have chosen to obtain a digital Islamic banking licence. FinTechs, on the other hand, are envisaged to continue to have an increasing influence on customers' experiences and expectations. For now, their influence may not be severe, for several reasons. These include regulatory barriers to entry, inertia to switch among many old customers, and the possibility of the incumbents using their financial capability either to replicate or to absorb the FinTech firm outright.

Nonetheless, the FinTechs have expanded the scope of their services beyond digital payments and e-wallets. They now offer Sharī'ah-compliant peer-to-peer (P2P) financing and equity crowdfunding, which are considered top growth sectors for the Islamic FinTechs in 2020.[63] This may exert pressure on the incumbent IBs' profitability and ability to weather future business cycles.[64]

Forty per cent of the respondent IBs strongly agree that the lack of government digital infrastructures poses a challenge for a smooth and rapid transformation of their digital activities. Such infrastructures include high-quality communication services that provide wide and affordable access to both internet and mobile connectivity. National platforms such as MyInfo[65] APIs in Singapore and Central Credit Reference Information System (CCRIS) in Malaysia are examples of such critical infrastructures.[66]

4.2 Regulation of Islamic Digital Banking

Technological advancement also presents new regulatory and supervisory challenges for the financial sector regulators. RSAs have been generally cautious about ensuring that a favourable disposition towards technological financial innovation does not infringe on financial market integrity and stability. As such, RSAs are adopting different regulatory approaches towards digitalisation of banking operations. Some are adopting a bespoke digital banking license which places restrictions on banks' physical presence, and focuses on financial inclusion without altering existing fundamental banking license requirements.

Some other countries are adopting a phased approach in which case a specific digital banking license for new entrants is issued but for limited initial activities while being able to do so without being subjected to, for instance, stringent regulatory requirements and huge capital investments. Another approach adopted in some countries is that where no specific digital banking license is issued in order to among other objectives encourage innovation in the financial service industry.[67]

---

[63] https://ceif.iba.edu.pk/pdf/IslamicFinTechReport19.pdf

[64] FSB (2019), *FinTech and Market Structure in Financial Services: Market Developments and Potential Financial Stability Implications*, p. 1: www.fsb.org

[65] MyInfo eliminates the need to repeatedly provide the same personal information when transacting online or for the purpose of electronic know-your-customer (e-KYC) for remote customer onboarding.

[66] CCRIS is a system created by Bank Negara Malaysia in which credit information about both existing and potential borrowers is provided in a standardised report format.

[67] Jenik, I, Flaming, M, and Salman, A. (2020) Inclusive Digital Banking: Emerging Case Markets Case Studies, CGAP/World Bank https://www.cgap.org/sites/default/files/publications/2020_10_Working_Paper_Inclusive_Digital_Banking.pdf pg. 40.

IBs were asked to describe the regulatory approach prevalent in their respective jurisdictions vis-à-vis the digital transformation process and developments. As shown in figure 4.2, in most jurisdictions, there are various regulatory approaches that are adopted in this regard. For instance, 32% of the respondent IBs indicate that specific digital banking regulations have been issued in their jurisdiction.

In Malaysia, Bank Negara Malaysia (BNM) issued the Policy Document on Licensing Framework for Digital Banks in December 2020 following a six-month public consultation. The licensing framework aims to promote innovative application of technology towards ensuring financial inclusion, financial well-being and sustainable growth while safeguarding financial system stability and customer protection. Up to five licences may be issued to qualified applicants where notification on the grant of license will be made by first quarter of 2022.

The licensing framework adopts a balanced approach to enable admission of digital banks with strong value propositions whilst safeguarding the integrity and stability of the financial system as well as depositors' interest. To achieve these outcomes, a simplified regulatory framework will be applied to digital banks during the initial stage of operations, commensurate with an asset threshold of not more than RM3 billion for three to five years, in the areas of capital adequacy, liquidity, stress testing, Shariah governance and public disclosure requirements. Digital banks will be required to comply with the Islamic Financial Services Act 2013 (for Islamic digital banks) or Financial Services Act 2013 (for conventional banks), as well as standards on prudential, Sharîʿah, business conduct, consumer protection and ML/FT.

The State Bank of Pakistan in December 2019 also issued a revised Branchless Banking Regulations for financial institutions in the country including Islamic banks.[68] The regulation which is applicable to all financial institutions including the IBs in the country provides details on what activities constitute branchless banking as well as serve as a set of minimum standards that need to be complied with by the banks desirous to offer branchless banking services. Aspects covered include overall information on matters relating to permissible models and activities, use of technology, security, customer protection and risk management etc.

A majority of respondent IBs (57%) indicated that there are ongoing efforts to amend the existing regulations in their jurisdiction to cater for the peculiarities of digital banking operations. Another 8% of the IBs mainly from Saudi Arabia indicate that although existing regulation remains unchanged, further clarity have been provided on how such regulation applies to digital banking operation. Only 3% IBs and mainly from Senegal indicated that digital banking regulation is not presently being considered in their jurisdiction.

In Saudi Arabia, additional licensing guidelines and criteria for digital-only banks were issued by the Saudi Central Bank (SAMA) in February 2020.[69] The guidelines complement SAMA's existing Banking and Licensing Guidelines and Minimum Criteria. The main intent is to promote a financial ecosystem that is driven by an innovative-based financial technology and which provides opportunities for fintech start-up banks.

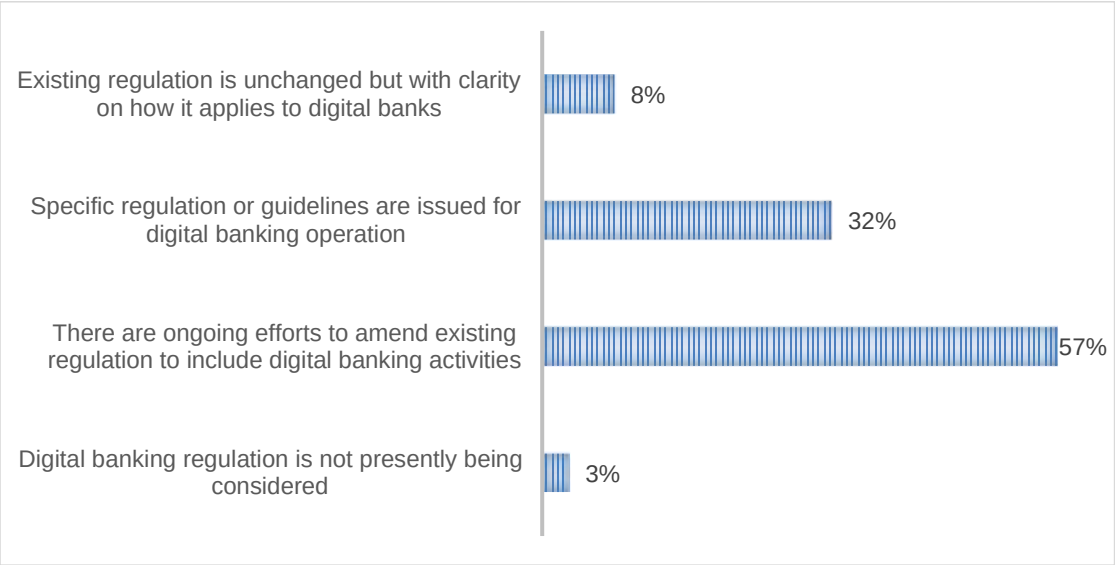
The SAMA licensing guideline also provides details on specific licensing conditions including relevant experience and knowledge, and the financial capacity of the founders. Specifics on other requirements are also provided including business plan, exit plan, capital adequacy assessment plan, and internal liquidity adequacy assessment plan. The operational

[68] https://dnb.sbp.org.pk/bprd/2019/C10-Branchless-Banking-Regulations.pdf
[69] https://www.lw.com/thoughtLeadership/SAMA-Issues-Additional-Licensing-Guidelines-for-Digital-Only-Banks-in-Saudi-Arabia

compliance set by SAMA for the conventional banks are also applicable to the digital-only banks.

In Indonesia, digital operations in banks are regulated by the Financial Services Authority regulation (POJK number 12/POJK.03/2018) especially regarding the risk management in the implementation information technology and digital banking services by commercial banks.[70] Digitising Islamic financial instruments is also a key component of the OJK's five-year financial master plan - MPSJKI 2021–25.

Figure 4.2 Regulatory approaches to digital transformation



Source: IFSB Survey, 2020

Jurisdictions where Islamic banking operates generally have one form or another of a regulation, policy document, rulebook, etc., that guides the application of these various technologies and mitigation against prudential risks that may result therefrom. Most of the respondent IBs indicated that these regulations are available on the websites of their respective RSAs.

About two-thirds (77%) of the IBs also responded that there are no specific digital banking regulations for IBs separate from those for the conventional banks. This is generally expected given that the various forms of technology being applied are meant to aid delivery of Islamic banking products and services without infringing on the tenets of the applicable Sharīʿah injunctions. It is the extra emphasis placed on Sharīʿah consideration that is adduced as the reason why the remaining 23% of respondents stated otherwise.

Some jurisdictions have also rolled out action plans for non-bank financial service providers, such as for Islamic FinTechs. Others have included technology companies within the purview of their macroprudential assessments in order to strengthen regulatory oversight on financial technology. Most have issued various regulations relating to cashless payments, electronic

[70] https://www.ojk.go.id/id/regulasi/Pages/Penyelenggaraan-Layanan-Perbankan-Digital-oleh-Bank-Umum.aspx

money institutions, cyber-security, electronic or pre-paid cards, crowdfunding, cloud computing, regulatory sandboxes and open banking.

Some countries are also considering monitoring the implications of third-party relationships that exist among various Islamic banks and their FinTech partners.[71] This is perhaps to mitigate against step-in risk, which may arise outside of, but is connected to, the Islamic banking industry.[72] This interconnection may arise through ownership, partnership or a sponsorship relationship between an incumbent and a financial service disruptor.

In Bahrain, the Central Bank of Bahrain's (CBB) Operational Risk Management Module sets out the regulation and general requirements regarding IBs' outsourcing, electronic money and electronic banking activities, as well as security measures. The CBB has also since 2017 issued various regulations regarding the application of technology in banking operations as well as crowdfunding and cloud computing. CBB also established a Fintech and Innovation Unit and a Regulatory Sandbox. The Regulatory Sandbox Framework sets out the CBB's approach to authorising Regulatory Sandbox Participants in the Kingdom of Bahrain. In 2018, in addition to issuing new regulations on open banking, both the regulatory sandbox and crowdfunding regulations were revised. In 2019, Crypto-asset regulation was issued, as well as regulation for digital financial advice. At the outbreak of COVID-19, the limit of NFC payments without PIN transaction has been increased and payment tokenisation rolled-out.

In September 2020, the Central Bank of the UAE (CBUAE) issued new regulation on Stored Value Facilities (SVF) with the main aim of supporting digital payment services in the UAE. The SVF is a facility, provided via cards, fund transfer, reward points, or crypto assets, and which allows a customer to pay a sum of money to the SVF issuer in exchange for the storage of that money on the facility. Although banks are exempted from the regulation, they are required to inform the CBUAE if they plan to carry out SVF activities. The regulation also provides guidance on scope of SVF activities, licensing requirements including financing, corporate governance, risks and security management, business continuity plan, customer protection and ML/FT control systems. A transition period of one year is provided in the regulation after which an assessment report is issued by an independent party on the compliance of the SVF operator with the regulation.[73]

In Saudi Arabia, in August 2020, SAMA issued an update to the Payment Services Provider Regulations (PSPR) which was introduced in January 2020 and applies concepts implemented by the European Union's Payment Services Directive (PSD2). The PSD2 makes it easy for international PSPs to launch operation in Saudi Arabia based on a familiar payments system concept. SAMA had earlier issued preliminary sandbox licenses which though comes with some restrictions nonetheless allowed payment service providers to test new digital solutions in a live environment. The regulation also provides information about the requirements for shareholding, management, business plan, and other disclosure requirements.[74]

In Malaysia, there is the Risk Management in Technology (RMiT) policy document issued by BNM. It sets out the BNM's requirements with regard to financial institutions' management of

[71] These regulatory frameworks and sandboxes are available on the website of the RSAs in various jurisdictions.
[72] X. Vives (2019), "Digital Disruption in Banking", *Annual Review of Financial Economics*, 11, 243.
[73] https://www.pwc.com/m1/en/tax/documents/2020/central-bank-uae-stored-value-facilities-regulation.pdf
[74] https://www.lw.com/thoughtLeadership/sama-updates-payment-services-provider-licensing-regime-in-ksa

technology risk and to prevent the exploitation of weak links in interconnected networks and systems that may cause detriment to the financial system.[75]

The Central Bank of Kuwait (CBK) in a bid to strengthen the cyber resilience of the banks operating in its jurisdiction issued the Cyber Security Framework for Kuwait Banking Sector in 2020. The framework provides details on the core principles for governance, risk management and compliance, collaboration, and continual improvement in cyber-resilience of Kuwait banking sector.[76]

The Central Bank of Sudan (CBOS) is implementing a Real Time Gross Settlement (RTGS) system as a key component in the reform of the National Payments System (NPS) towards contributing to the efficient operation of the financial system in the country. It is expected to enhance liquidity, increase security of payment processing, reduce associated risks, and to promote efficiency in terms of speed, cost and robustness. It provides a mechanism for participants to settle large value and time critical payments in many regards.

The Central Bank of Egypt (CBE) has issued general principles and basic instructions on Digital Banking "FinTech". CBE has also launched its FinTech and innovation integrated strategy to enhance digital transformation. Similarly, in the Kyrgyz Republic, various regulations have also been issued relating to cashless payments by the National Bank of the Kyrgyz Republic (NBKR).[77] In Brunei Darussalam, a digital payment roadmap has also been issued to transform the payments environment through promoting digitization, issuing regulatory framework, ensuring greater acceptance and usage, integrating with regional payment systems and ensuring interoperability.[78]

SECTION 5: FINANCIAL STABILITY IMPLICATION OF THE DIGITAL TRANSFORMATION OF IBs

Without prejudice to the numerous benefits that digital banking offers, it has resulted in increased activity by non-bank financial institutions,[79] as well as increased cyber-security risks,[80] among other operational developments. Technological adoption has brought about a new regulatory and supervisory challenge for the financial sector regulators as new risks are introduced – for instance, safeguarding data privacy,[81] cyber security, consumer protection, consumer financial health, compliance with anti-money laundering/combating the financing of terrorism (AML/CFT) regulations, and so on.

In terms of the financial stability implications of digitalisation, 78% of the responding IBs indicated that positive competition would be heightened due to the entrants of disruptors. This would reduce concentration in the Islamic banking industry, especially if regulatory guidance and the requisite infrastructure allow new entrants to leverage on technology to unbundle financial services as well as increase contestability.

[75] https://www.bnm.gov.my/index.php?ch=57&pg=137&ac=813&bb=file
[76] https://www.cbk.gov.kw/ar/images/csf-feb-2020-1_v00_tcm11-148304.pdf
[77] https://www.nbkr.kg/index1.jsp?item=106&lang=RUS
[78] https://www.ambd.gov.bn/Site%20Assets%20%20Slider%20Home%20Page/DPR%202019-2025.pdf
[79] Ibid, 243–72.
[80] Concerns about cyber-security risks featured prominently in the response to the CIBAFI's Global Islamic Banking Survey 2019: http://cibafi.urbansoft.co.uk/Files/L1/Content/CI1809-CI1809-GlobalIslamicBankersSurvey2019Report.pdf
[81] There is a need to ensure that digital footprints generated are not used to expose customers to the threat of security risks such as digital fraud and abuse, or "emotional manipulation" arising from unsolicited suggestions to purchase other products and services.

Perhaps new entrants, in a bid to avoid regulation and compliance costs, would opt not to become licensed Islamic digital banks, so would not be able to venture into activities such as accepting deposits.[82] The fact that the new entrants do not perform liquidity transformations means that, as per e-money regulations, clients' funds would have to be placed at their disposal – for instance, as deposits in the IBs. This presents a competitive advantage to incumbent IBs due to the opportunity it provides for them to obtain stable and cost-efficient funding.

Other factors include reputation and brand recognition, and the possibility of the incumbents using their financial capability either to replicate or to absorb the new entrants outright.[83] The COVID-19 pandemic has also resulted in a significant pull-back of venture capital investments in FinTechs, causing many of them to be faced with the challenge of coping with abrupt pressure to maintain operational resilience even as the economic uncertainty may stunt their growth trajectory.[84]

If properly executed, digital transformation holds opportunities for IBs to boost their revenues.[85] Nonetheless, the new entrants are envisaged to continue to have an increasing influence on customers' experience and expectations. This may exert pressure on the incumbent IBs' profitability, especially in profitable lines such as payments, thus constraining their ability to weather future business cycles.[86] This view is agreed to by 61% of the IB respondents, who also stated that the incumbents may resort to increased risk taking to make up for the shortfall in margins.[87]

In order to curb excessive risk taking at the individual bank level and systemic risks at a macro level, prudential requirements have often been imposed on incumbents. For instance, to complement the Basel III accords, there are equivalent IFSB standards on capital adequacy and liquidity requirements for IBs that have been implemented in numerous jurisdictions. However, by imposing prudential regulations, the impetus for shadow Islamic banking activities may increase, as has been observed in conventional banking. Shadow banks[88] as financial service disruptors have been said to prosper in areas and activities where compliance with regulatory requirements has been considered a burden by traditional deposit-taking banks.[89]

Sixty-five per cent of the respondents supported the view that the regulatory challenge in balancing the objectives of facilitating innovation while ensuring financial stability inhibits the provision of a clear policy guideline. Moreover, a lack of, or unequal application of, regulation on, for instance, prudential requirements may encourage regulatory arbitrage and higher risk taking by new entrant disruptors. The inertia that inhibits provision of a clear policy guideline in

[82] As stated in the *Islamic Fintech Report*, 2018, out of the 93 Islamic FinTech start-ups, only eight focused on deposits and transfers.
[83] Ibid.
[84] N. Uwaje (2020), Presentation made at the Arab Monetary Fund (AMF) online meeting on "FinTech Innovation, Regulations and Collaboration: FinTech Resilience during and post COVID-19", held on 7 May 2020.
[85] For instance, in Malaysia, Bank Islam's multi-year digitisation programme resulted in 80% y-o-y growth in internet banking related fee income, 25% y-o-y growth (to 1.2 million) in the number of users, and a 133% growth in online transactions in 2018. See https://themalaysianreserve.com/2019/07/08/digitising-to-drive-growth-of-islamic-banks/
[86] FSB (2019), *FinTech and Market Structure in Financial Services: Market Developments and Potential Financial Stability Implications*.
[87] Profitability is a significant predictor of financial crises and the resilience of banking institutions. As an important determinant of retained earnings, it serves as the first line of defence in the event of financing losses or impairment.
[88] These institutions provide partial or full financing intermediation outside the regular banking system.
[89] Buchak et al. (2018, cited in Vives, 2019) stated that approximately 55% of the growth in shadow banking could be attributed to the regulatory difficulty faced by traditional banks.

this regard could also magnify the threat to financial stability. This view is supported by 88% of the respondent IBs.

The fact that these new entrants help to mobilise a substantial amount of funds, which they do not retain, may heighten their susceptibility to moral hazards and adverse selection due to information asymmetry.[90] There are also arguments that the new entrants, in a bid to increase financing volume to boost revenue, may result in a lower-quality financing assessment process.[91] This view is supported by 58% of the respondent IBs.

In the medium to long term, however, these new entrants,[92] and other non-bank players such as TechFins,[93] are expected to be the pivot around which the changing landscape of the financial ecosystem, including the IFSI rotates. A widely held view is that the future of financial services will be shaped by how much control customers have over the data held about them by financial institutions, and by how much access third parties have to this data. In this case, Islamic FinTechs are also expected to accelerate their entry into prominence in the Islamic banking and financial ecosystems.

The gradual shift among financial institutions from an on-premises data service to a public cloud-based data service makes subscribing to an external third-party cloud service provider inevitable. The potential is high for a systemic risk to be triggered by cloud concentration risk due to the operational centrality of computing services.

Furthermore, the FSB already notes the financial stability implications of banks not having control or ownership of their data hosted on cloud platforms, especially if there is a cyber-attack on or an operational failure of such cloud services.[94] In response to a related question in the survey, 66% of the IBs consider that an attack on, or operational failure of, the main cloud service providers to an IB will have financial instability implications for their operations.

Essentially, RegTech and SupTech[95] in Islamic finance are aimed at enhancing the transparency, consistency and standardisation of regulatory processes. This is in a way that promotes proper interpretation of regulatory standards and at a lower cost and ensures risk-based supervision for Islamic banks' regulators. The role for regulators in this space would be to ensure that huge investments are made in technology to enhance the automated analysis of examination and enforcement of Islamic banking principles. It is envisaged that the consequential enhanced regulatory compliance, monitoring of activities and improved real-time surveillance would have positive implications for the stability of the financial system

Furthermore, discussions around central banks creating their own digital currency are gaining traction, especially due to the outbreak of COVID-19 which has further amplified the need for contactless payments. Such central bank digital currencies may be used as a means to

[90] For instance, based on the *mudārabah* financing mode adopted in Islamic equity crowdfunding, only the investors bear the loss of capital to the extent that the crowdfunding service provider is not negligent.
[91] Bayluk and Davydenko (2018, cited in Vives, 2019) stated that P2P loans recorded higher default rates relative to other types of credit among consumers of comparable scores.
[92] According to the FSB (2019), *FinTech and Market Structure in Financial Services: Market Developments and Potential Financial Stability Implications*, these are "technology-enabled innovations in financial services that could result in new business models, applications, processes or products with an associated material effect on the provision of financial services".
[93] These firms leverage on their technological advantages and possession of data about a large number of their pre-existing customer base while rendering their primary business. On the basis of these dual advantages, they add rendering financial service to their value chain.
[94] R. Harmon (2018). "Cloud Concentration Risk: Will This be our Next Systemic Risk Event?", Cloudera White Paper: https://www.researchgate.net/publication/331099204_Cloud_Concentration_Risk_Will_this_be_our_next_Systemic_Risk_event
[95] RegTech is the use of technology by financial institutions to enhance compliance with prudential regulations, while SupTech is the use of technology by RSAs to enforce prudential regulation.

complement monetary policy toolkits to tackle susceptibility to recession by getting financing across vulnerable businesses and households. Without prejudice to its benefits, what is being debated is the profound implications such currencies will have for the profitability of banks, especially in this stressed period.

SECTION 6: CONCLUSION AND RECOMMENDATION

6.1 Conclusion

The adoption of innovative technologies and business models is a prominent emerging trend that is fast changing the ecosystem of the IFSI, and Islamic banks are not immune to these developments. Emerging technology is expected to further revolutionise the financial sector, and enhance financial inclusion, accessibility, convenience and efficiency. Both competitors and competition are changing and the IBs need to respond accordingly through technology.

The rationale for IBs' digital transformation drive is informed by a plethora of reasons mainly to enhance their competitiveness and contestability in the IFSI via operational efficiency and modernisation of their business model. This is in response to the disruption of financial services rendering by new entrant Fintech start-ups as well as competition from incumbent IBs. This would entail that the IBs leverage on technology to increase customer value and satisfaction, reduce operational cost, enhance revenue generation, strengthen core competences, and improve data security, among other considerations. However, this should be done without infringing on the fundamentals of the Sharīʿah.

The COVID-19 outbreak and the consequential movement restrictions and physical distancing as measures to flatten the curve of its spread have added to the need for digitalising financial services, including those offered by the IBs. For instance, most of the IBs have also adopted the work-from-home policy, which requires remote access and strengthening of the security of their technology network.

More than two-thirds of the IBs are at various stages of their digital transformation process. While the specific status of their implementation varies, it is promising to know that they have commenced. However, most of the IBs in this category are also those that expended less than 50% of their most recent budget on IT-related activities. Those few IBs that commenced their digital transformation process prior to the outbreak of COVID-19 are expected to find it relatively easier than those that would have to react due to the inevitability of such transformation as a crucial post-COVID-19 economic recovery reality.

Mobile technology/digital wallets and the use of biometric authentication are the most commonly adopted technologies by the IBs. Plausible reasons could be their usefulness, especially for financial inclusion through payment services and financing, especially during COVID-19. Moreover, both technologies can be applied via smartphones, the use of which is quite common among IBs' customers. These two technologies, in addition to security and privacy technologies, are those on which the larger chunk of IBs' IT budgets are expended.

APIs are also very common among the IBs, due to its data-sharing and analytics possibilities. Cloud computing has also been very much deployed, especially for unbundling of services and for data sharing in open banking applications. The adoption of robo-advisory and blockchain technology for smart contracts is, however, still in the very early stages.

Cyber security is the main prudential risk facing IBs in their digital transformation activities. Also notable are technology risk, data integrity risk, third-party outsourcing risk and vendor lock-in risk. Although the IBs are faced with issues of legacy infrastructure, technical debt risk is not a primary concern. Also, digital Islamic banking operations are not considered to pose a direct Sharīʿah non-compliance risk. However, IBs' susceptibility to such risk through, for instance, system error is duly noted.

In most jurisdictions where Islamic banking is practised, there are no specific digital Islamic banking regulations. However, most jurisdictions have issued one or another form of regulation, policy document, rulebook, etc., that guides the application of these various technologies. There are also ongoing efforts in most jurisdictions to amend their existing regulations in line with technological developments.

The COVID-19 pandemic and the resulting lockdown revealed considerable scope for operational and supervisory improvements. For example, real-time monitoring of IBs is essential when a crisis unfolds rapidly. Digital tools could help in that respect. Similarly, supervision is to some extent still paper-based. This can be an issue for supervisors that may need to work remotely. The crisis has shown the need to set up systems so that future supervision can be carried out in a paperless fashion.

Legacy infrastructure that impedes quick and innovative responses to changing market needs is the main impediment to IBs' digital transformation. Budgeting constraints, as well as the lack of human capital (especially domain specialists), may slow the pace of digital transformation of Islamic banking. It is important to note that, in most jurisdictions, government continues to provide requisite supports and infrastructures such as technology hubs, national identity and APIs, which are crucial for open banking initiatives and architecture.

Digitalisation of the operations of IBs has implications for the financial stability of the IFSI in terms of how the incumbents respond to the digital transformation process and its consequential increased possibility for new disruptors to enter the market, thus heightening competition. Such responses would also reflect on related issues such as cyber security, consumer protection, consumer financial health, compliance with AML/CFT regulations, and so on.

6.2 Recommendations

Regulators in jurisdictions where Islamic banking is practised have, and are continuing to roll out, requisite policy guidelines and frameworks, as well as promoting regulatory sandboxes, etc. Nonetheless, as events unfold, further consideration needs to be given to how a robust regulatory framework can be maintained to ensure that technological innovations are pursued without adversely impacting financial stability and achieving support for financial inclusion and real economic growth.

RSAs need to be cognisant of the potential new risks that digital Islamic banking poses as they coordinate prudential regulation and competition policy. Developing a "fit-for-purpose" regulatory and supervisory regime is imperative, notwithstanding the formidable challenge it presents in balancing the objectives of facilitating innovation while ensuring effective risk management and financial stability. In this regard, regulators are expected to increase their attention on both entities and activities given the diverse groups that are involved in the digital transformation process. RSAs will also need to increase the frequency of simulation exercises

on emerging technology risks and to strengthen their focus on internal cyber-security activities by requesting data on cyber threats.[96]

As new risks are introduced, safeguarding data privacy, cyber security, consumer protection, consumer financial health, compliance with AML/CFT regulations, and so on, would require that those regulations are up to speed. In order to strengthen regulatory oversight on financial technology, RSAs may consider monitoring the implications of third-party relationships that exist among various IBs and their FinTech partners, perhaps to mitigate against step-in risk that may arise outside of, but connected to, the Islamic banking industry.[97]

It is essential to ensure that technology-led operations duly comply with Sharī'ah governance requirements to ensure best practices while protecting consumer rights. An effective Sharī'ah governance system for maintaining Sharī'ah compliance is the core of the Islamic banking business that differentiates it from conventional banking regardless of the platform through which products and services are provided.

Government support for the digital transformation process has been very encouraging in numerous jurisdictions where Islamic banking is present. This is through providing guiding policy documents, a conducive environment and the infrastructure needed for regulatory sandbox experiments.[98] Building on experiences garnered specific to digital Islamic banking regulatory guidance on conduct requirements and operational matters relating to risk, data management, product and process compliance with Sharī'ah, etc., is necessary to create justification for the distinct identity from the conventional digital banks. It should also be possible to support Islamic FinTechs in developing partnerships with the IBs, or providing a conducive regulatory environment for IBs to assist the growth of Islamic FinTechs.

Human capital development is a fundamentally important pillar for innovation to be successful. The digital transformation process requires highly specialised human capital and domain experts both for operation and regulation. Therefore, both regulators and providers of digital Islamic financial services will need to retrain and reskill existing talent even as they make efforts to attract new talents that fit the imminent transformation of the digital banking workforce.

The IFSB has a dedicated segment to digital finance in its Technical Notes on Financial Inclusion.[99] In this document the IFSB provides detailed technical guide on the priorities and consideration that are pertinent for regulatory and supervisory oversight vis-à-vis the implication of technological innovation for financial inclusion through the Islamic financial services industry of member jurisdictions. Similarly, the IFSB Guiding Principles for Investor Protection in Islamic Capital Markets also provide details on how to ensure the application of technology in providing Islamic financial services without infringing on client protection and financial stability.[100]

[96] Examples from conventional banking – including efforts such as the Cyber Security Fortification Initiative in Hong Kong, and the centre established in Singapore to monitor cyber threats to firms – are expected to continue in numerous other jurisdictions.
[97] X. Vives (2019), "Digital Disruption in Banking", *Annual Review of Financial Economics*, 11
[98] This requires providing support for critical infrastructure and ancillary services available to FinTechs, such as incubator centres, office spaces and other "hard" infrastructure. This may also require governmental support through tax incentives and other schemes that may attract Islamic FinTech start-ups. Examples of the regulatory sandboxes of the UAE, Bahrain, Malaysia, etc. are worth highlighting in this respect.
[99] IFSB (2019) TN-3 Technical Note on Financial Inclusion and Islamic Finance. https://www.ifsb.org/download.php?id=5519&lang=English&pg=/published.php
[100] IFSB (2020) IFSB-24 Guiding Principles on Investor Protection in Islamic Capital Markets. https://www.ifsb.org/download.php?id=5918&lang=English&pg=/published.php

At the moment, perhaps, there may not be an urgent need for standards on financial technology. Standards or regulations are principles-based, whereas most of the activities around machine learning and artificial intelligence, for instance, are based on algorithms built around big data. As such, the pace of disruptive technology may be too fast for a standard development process, thus exacerbating the exposure of IBs to the vagaries of the pervasive technological disruption. In this case, a role for international standard setters such as the IFSB[101] would be to observe and share best practices and case studies as a form of general principles across jurisdictions while engaging in innovative collaboration with other international standard setting bodies.

[101] As per its mandate, the IFSB sets prudential standards for institutions offering Islamic financial services to complement other international standard setters such as the BCBS, IOSCO and IAIS.

Appendix

Number of Respondent IBs by Country

Countries where respondent Islamic bank is based	**Number of respondent Islamic banks**
Bahrain	7
Bangladesh	6
Brunei Darussalam	3
Egypt	1
Indonesia	3
Jordan	5
Kuwait	5
Kyrgyz Republic	1
Malaysia	3
Morocco	1
Nigeria	3
Pakistan	14
Philippines	1
Qatar	1
Saudia Arabia	2
Senegal	1
Singapore	1
Sri-Lanka	1
Sudan	1
Turkey	1
United Arab Emirates	18
21 countries	**80 Islamic banks**