

Article

Strengthen the Security Management of Customer Information in the Virtual Banks of Hong Kong through Business Continuity Management to Maintain Its Business Sustainability

Haosheng Chen ¹ , Daniel Tse ^{2,*} , Pengfei Si ², Gefei Gao ² and Chang Yin ²

¹ College of Engineering, City University of Hong Kong, Kowloon, Hong Kong 999077, China; haoshchen2-c@my.cityu.edu.hk

² College of Business, City University of Hong Kong, Kowloon, Hong Kong 999077, China; pengfeisi2-c@my.cityu.edu.hk (P.S.); gefeigao2-c@my.cityu.edu.hk (G.G.); changyin2-c@my.cityu.edu.hk (C.Y.)

* Correspondence: iswktse@cityu.edu.hk

Abstract: This article looks at studies on how to use business continuity management for Hong Kong's virtual banks in order to reduce customer information risks, so as to maintain business sustainability. Firstly, the development of virtual banks in Hong Kong were investigated, the laws and regulations and regulatory policies of Hong Kong and the Mainland were benchmarked, and the main risks that may occur and be harmful to the bank business sustainability were analyzed. Considering the characteristics of virtual banks, the main concerns of public customers about the IT risks of virtual banks through questionnaire surveys were collected and analyzed. Moreover, the importance of business continuity management to virtual banks was drawn. Secondly, in the case studies, via understanding the overall situation of WeBank, its performance during the COVID-19 pandemic, and the regulations of the Monetary Authority of Singapore, the practice standards of virtual banks in business continuity management were further clarified. At the end, three suggestions for virtual banks in Hong Kong were put forward to reduce customer information security risks through business continuity management, thereby maintaining its business sustainability.

Keywords: virtual banks; business continuity management; business sustainability; security management; customer information



Citation: Chen, H.; Tse, D.; Si, P.; Gao, G.; Yin, C. Strengthen the Security Management of Customer Information in the Virtual Banks of Hong Kong through Business Continuity Management to Maintain Its Business Sustainability. *Sustainability* **2021**, *13*, 10918. <https://doi.org/10.3390/su131910918>

Academic Editor: Giuliana Birindelli

Received: 11 August 2021

Accepted: 27 September 2021

Published: 30 September 2021

Publisher's Note: MDPI stays neutral with regard to jurisdictional claims in published maps and institutional affiliations.



Copyright: © 2021 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<https://creativecommons.org/licenses/by/4.0/>).

1. Introduction and Background

Although virtual banks (VB) in Hong Kong have operated for several years, many risks have not been completely prevented and controlled, which may be detrimental to its business sustainability. Aiming at the possible risks of virtual banks in customer information security and business sustainability, in-depth analysis and discussion on the potential problems and solutions of virtual banks in the face of disaster events were conducted. Based on the theory of business continuity management, this research plans to develop some comprehensive and feasible safety management prevention and control optimization measures for virtual banks to maintain their business sustainability. Business continuity management (BCM) is of crucial importance to the protection mechanism for disaster prevention in the financial industry. It is often referred to as one of the most effective plans in the face of crises, incidents, and disasters, especially concerning the plans for the organization to continue or resume operations. With financial institutions paying increased attention to the construction of BCM and business sustainability in order to make BCM more suitable for virtual banks in the future, this research further explored and analyzed some of the best practice for daily operation.

The informatization construction of financial institutions has developed rapidly, and the degree of informatization is also becoming more and more popular. Information security risk management has become an increasingly important process in modern businesses

(Bojanc, R., and Jerman-Blažič, B., 2013) [1]. The financial industry suffers a significant increase in losses in the face of disaster events, and its demand of business sustainability and the dependence on the stable operation of the system in daily business operations also increase significantly. Progress in information technology has brought significant changes which resulted in the emergence of a new type of banking called virtual banking (Ahmadalinejad, M., and Mohsen Hashemi, S., 2015) [2]. The virtual banks have not only faced the same credit market and interest rate risks as traditional banks, but also its risks in information security, liquidity, sustainable development, and operations may intensify due to their all-day business nature. Information security risks, in particular, are of vital importance to virtual banks. Once the data center of the virtual bank has a risk of information security, such as security loopholes or unauthorized intrusion leading to information systems running slower or being interrupted, this will cause huge economic losses and reputation losses, or even lead to the financial system becoming paralyzed. As a result, business sustainability will be affected substantially.

If a company loses 20 MB of vital business data, it will lose USD 17,000 in sales, USD 19,000 in finance, and USD 98,000 in technology management (Qu Xingquan, 2020) [3]. Therefore, virtual banks should carry out security management and prevention in a timely manner. Especially in the event of information security hazards, virtual banks should ensure the normal operation of the information system, or be able to recover in a timely manner after the interruption, reduce the property loss and social impact brought to the people after the disaster so as to avoid financial disorder. This has become an important research direction in the sustainable operation and management of a virtual bank's information system.

In this research, first of all we used quantitative methods to find out whether the consumers have concerns on the reliability of virtual banks and whether the virtual banks are highly aware of the importance of business continuity. Based on those findings, we used two case studies to explore the nature of the problems affecting virtual banks' business continuity and finally derived three recommendations for strengthening virtual banks' security management through BCM.

2. Motivation and Methodology

2.1. Research Motivation

Hong Kong is now one of the biggest international financial centers. Its success relies on its well-established economy, financial system, and regulation. Introduction of virtual banks' operations may be a threat or an opportunity, hence the study of its relevant information security risks associated with virtual banks are of paramount importance. Thus, our research motivation of studying the virtual banks in Hong Kong is based on the following factors.

(1) The economy, finance, and the regulation in Hong Kong

A virtual bank (VB) is a bank which operates via electronic channels offering banking services. In the past, the general view of VB is that VB is a kind of service provided by the banks or financial organizations which have physical sites, such as virtualbank.com (accessed on 15 September 2021) by First Horizon Bank [4], but now all virtual banking services can be performed online and there is no more physical branch. In Hong Kong, virtual banking is a new service. The establishment of a virtual bank in Hong Kong is the beginning of the establishment of a healthy financial ecosystem. Competent participants attracted to this field will embrace the huge opportunities presented by challenging Hong Kong's traditional banking model in combining banking and technology (IFEC, 2019) [5].

The Hong Kong Monetary Authority (HKMA) published the Guideline on Authorization of Virtual Banks as early as 2000 [6], thus Hong Kong is the region that started to attach importance to virtual banks relatively early on in the world. It is believed that the growth of the virtual bank industry will stimulate local financial technology in the field of smart banking, which will strengthen Hong Kong's status as an international financial center, under the related authorization guidelines. The HKMA granted official licenses to

the local virtual banks for three consecutive months in 2019 [7], which indicates that Hong Kong's virtual banks have a strong official support.

(2) Risks in Hong Kong's virtual banks

The integration of banking and innovative technology has brought new risk appetite for virtual banks, which may do harm to the business sustainability. First of all, when managing the personal data of customers placed through the hosting systems supervised by the personal data collection ordinance on a virtual private cloud, virtual banks will face privacy data issues. In addition, outside of Hong Kong, the use of cloud technology can cause cross-border data transfers. Lastly, the participation of third parties may increase the probability of cyberattacks and cybercrimes. Hence, in using virtual banks, it is recommended to ensure a high level of IT system and network availability, perform regular IT system assessments and ensure business continuity, thus, to ensure its business sustainability. Meanwhile, many other risks have not been perfectly prevented and controlled in the virtual banks in Hong Kong, which may be detrimental to its business sustainability.

Moreover, the business continuity management (BCM) processes are integrated management processes for enterprises and institutions. The processes enable enterprises to recognize potential crises and related impacts, and to formulate strategies, plans and arrangements for risk response and business continuity recovery as well (Ma, W, 2014) [8]. The main goal of BCM is to improve the company's risk prevention capabilities to effectively deal with unexpected business interruptions and mitigate adverse effects. Briefly speaking, this empirical research can help virtual banks in Hong Kong understand the current risks and effectively prevent and control risks through reasonable BCM, thereby enhancing the information security and the business sustainability of virtual banks, which has certain practical significance.

2.2. Research Methodology

This research makes use of both qualitative analysis and quantitative analysis. Such a combination can let us more accurately understand the concerns of virtual banks' public customers, as well as conducting targeted benchmarking and providing proposals. Through questionnaire surveys it is possible to quantitatively collect and judge public customers' attitudes towards virtual banks and their key concerns about IT risks, while case analysis is able to find suitable cases for analysis from a qualitative perspective, so as to obtain targeted results, which eventually gives rise to appropriate conclusions.

In this regard, as shown in Figure 1, we mainly adopted desktop research, questionnaire surveys, and case study analysis methods, and give some suggestions on the continuity and sustainability management of IT risk for the virtual banking industry in Hong Kong.

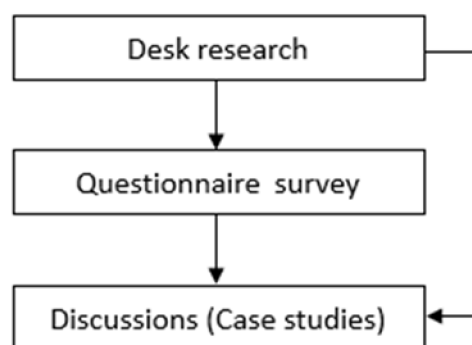


Figure 1. Research method.

Firstly, the desk research method allows us to quickly understand the development of the virtual banking industry and its potential IT risks. We conducted preliminary data research on the development of virtual banks, BCM, and banking business sustainability,

collect literature, inquire about industry regulations in Hong Kong, and outline the industry requirements and IT risks of virtual banks.

Secondly, the questionnaire survey method provides a quantitative and more convincing method to find the IT risk points that virtual bank control measures should firstly be focused on. From the public perspective, we learned about the public's concerns about virtual bank IT risks through questionnaire surveys and use statistical methods to classify the problems and find the major factors that virtual banks should pay more attention to.

Finally, the case study method, by means of a comprehensive study from local and overseas cases or regulations, can give the most direct reference for BCM of virtual banks in Hong Kong to maintain their business sustainability. We analyzed typical industry cases and their management methods to mitigate the impact of IT risks, combined with Hong Kong's more special operating environment, to analyze the IT risks that virtual banks of Hong Kong face and the methods they deal with.

3. Literature Review

The key focus point of this research is enhancing the protection of users' information in Hong Kong's virtual banks via utilizing the business continuity management to maintain its business sustainability, those users may be in Hong Kong or not. Hence, the key to this research ought to figure out the users' main anxieties to the virtual banks and the COVID-19 influence on the banking service and be supported by the risk management technologies and some official policies and regulations. Hence, we should review some literature about customers' concerns on the virtual banks, COVID-19 effects on the banking service, BCM, banking business sustainability, virtual banks' information risk management, and regulations on virtual banks to strengthen the security of virtual banks. A summary is created as follows:

3.1. Customers' Concerns on the Virtual Banks

As the virtual bank is an emerging and disruptive technology in daily life, people's acceptance of virtual banks is vital for its development. The virtual bank is a kind of internet bank, thus the concerns of the customers in the internet banks are worth being considered. Banking service quality and convenience, website availability and usability, bank information security and privacy, and perceived trust of internet banks are the key issues that the internet bank customers pay attention to, where website availability and perceived trust are the most significant problems they focus on (Aboobucker, I., and Bao, Y., 2018) [9].

Moreover, all of the services provided by the virtual bank are offered to its customers via electronic channels, such as the official websites and the APPs in smart phones and PCs, thus the virtual bank can be regarded as an e-banking service. Due to the fact that the virtual bank has no physical branches, the service quality of its electronic channels is particularly important for its brand. In addition, the service quality, the banking system security, and the cloud services have positive effects on customer satisfaction in the field of e-banking services, and customer satisfaction and loyalty have a significant contribution to the banks' profitability (Li, F., Lu, H., Hou, M., Cui, K., and Darbandi, M. 2021) [10].

Based on the customers' concerns and its impact on the virtual banks, the quality and the security of the virtual bank services are demanded to be concentrated on. Moreover, the availability and the usability of the virtual bank services are related to the continuity and the sustainability of the bank services. Therefore, regarding to the customers' attentions, it is required to reinforce the virtual bank information service quality to maintain its sustainability.

3.2. COVID-19 Effects on the Banking Service

The COVID-19 pandemic has precipitated devastation in every sector of the world; many industries involved in the area of information systems (IS) also have no escape. Under the circumstances of COVID-19, many business processes have been changed to

meet the requirements of emergencies; for example, normal work has been transformed to online mode, the workplaces have turned into people's homes (working from home), and many cutting-edge technologies have been applied and implemented for remote work. As a result, people need time and energy to study the relevant technologies, to adapt the new working style, and to balance the relationship between families and their work. Furthermore, some IS-related financial service companies also found that some of their business processes have to be restructured to fit virtual work (Conger, S., 2020) [11].

As a class of IS-related financial service organizations, the banks have also suffered from a great deal of damages in the catastrophe. For instance, in Zimbabwe, many banks operating brick and mortar branches have been in trouble since the start of 2020 (Muparadzi, T., and Rodze, L., 2021) [12]. Moreover, regarding the First State Bank on Sohu (2020) [13], the Federal Deposit Insurance Corporation (FDIC) announced on 3 April 2020, that the First State Bank in West Virginia has closed down. This was also the first bank in the United States to fail since the outbreak of COVID-19, which shows that the bank was unable to secure its business sustainability.

In short, the COVID-19 pandemic has caused a great many inconveniences to the IS-related industry, including the bank services. Thus, for the virtual banks in Hong Kong, it is critical to take some measures in business process continuity to prepare for such unexpected disasters to reduce the loss, to enhance the organizational sustainability and the work efficiency.

3.3. Business Continuity Management

Most of the studies about the quantitative research on the business process strategy only focus on the normal circumstances, yet few of them are involved in the business disruption situations. However, when facing the unstable conditions such as the COVID-19 pandemic, the lack of the attention or the construct for the business turbulent period will leave the firms (such as virtual banks) vulnerable, and may even be destroyed by the sudden disasters and crises (Miao, M., Saide, S., Ratna, S., and Muflih, M. 2021) [14]. Hence, it is necessary to adopt some business continuity innovative measures which are able to retain the continuity and sustainability of the business processes, such as the business continuity management.

The general definition of business continuity management (BCM) is a series of executive processes that identify potential menaces to the organizations and the impact that these menaces may have on the business operations of the organizations if they occur (Zhang X., Han S. and Xie Z, 2019) [15]. For defending the organizations' profits, reputes, business sustainability, and value-creating activities of key stakeholders, BCM offers a framework for organizations to establish an effective self-recovery ability to respond to threats (Ma, W, 2014) [8].

Moreover, the essential elements of BCM are the components of organizational tactical management, the advance recognition of the potential threats, the early resilience establishment, the program and the review of the strategies to the consequences of the damage, as well as a risk managerial method (Muparadzi, T., and Rodze, L. 2021) [12]. Therefore, BCM's key factors' application and its effectiveness is crucial to the continuity and the sustainability of the organizations' business processes.

Additionally, in accordance with the content about BCM from Baidu baike (2020) [16], the main purpose of BCM is to enhance the enterprise's risk prevention powers to avaiably respond to unexpected business disruptions and to reduce adverse effects. The basic principles of BCM are to ensure that the core business operations of the institutions involved can always continue to move on, and the most popular basic methods of BCM include establishing a business continuity management system (BCMS). Moreover, BCM is also conducive to a variety of project activities, such as performing business impact analysis and risk analysis, conducting assessments, and developing business continuity (BC)/disaster recovery (DR) plans, and so on.

Furthermore, BCM pre-planned business interruption scenarios to make preparations for virtual banks if its key processes fail. By identifying hazards exposed to internal and external risks, the BCM process can increase the resilience of the organization, which develops the capability for effectively responding to threats such as natural disasters or data breaches and protecting business interests as well as the business sustainability of the organization.

In summary, the implementation of BCM is able to strengthen the information security of the customers in virtual banks of Hong Kong to conserve its business sustainability.

3.4. Banking Business Sustainability

As per the press “HKMA introduces key measures on sustainable banking and green finance” from the Hong Kong Monetary Authority (HKMA, 2019) [17], business sustainability is an essential requirement for banking development. Typically speaking, banking business sustainability is the possibility and ability of a bank to maintain productivity and survive in the future. In a sense, it usually refers to the sustainability of a bank in developing its business, maintaining connections with old customers, and discovering new customers, thus it usually involves customer loyalty and the way in which bank leaders manage the bank. Customer loyalty is a vital part of a company’s sustainable development because it can not only create repeat business, but also create new business, and the customers’ satisfaction will also aid the bank’s reputation growth. Hence, many banks use different plans and initiatives to increase customers’ satisfaction and loyalty to ensure safe and continuous business sustainability.

However, the virtual bank has no offline branch as it is a type of non-contact bank. From the article “Lay a firm foundation for the sustainable development of non-contact banks” (Li, G, 2020) [18], after the COVID-19 pandemic, the customers’ dependence on the non-contact banks will decrease, and some are not as safe, but convenient measures for banks to deal with COVID-19 may no longer apply, and the customers’ awareness of banking security will also raise. As a result, customer loyalty and connection will reduce, and virtual banks are also facing many information risks, which are pernicious to banking business sustainability.

Moreover, BCM is a valuable way to enhance the bank’s information risk prevention ability in order to win the trust of the customers and thereby holding customer loyalty, which is profitable to banking business sustainability. Therefore, we can use it to help virtual banks in Hong Kong maintain business sustainability.

3.5. Virtual Bank Information Risk Management

It is widely understood that the integration of banking and emerging technology gives virtual banks a new risk profile (Bryan Cave Leighton Paisner, 2018) [19]. First, with the adaptation of open application programming interfaces (APIs) and third-party collaborations (such as hosting systems on virtual private clouds), when managing the personal data of customers that are enforced under the personal data (privacy) regulations, virtual banks will enjoy privacy data issues. Furthermore, the use of cloud technology outside Hong Kong may result in cross-border data transmission. It is recommended that virtual banks do not transfer any customer’s personal data to places outside Hong Kong without the customer’s permission. Moreover, there are numerous major elements in using cloud technology, such as the cloud implementation cost, cloud data confidentiality, the capacity of the bank in the cloud application, as well as the bank leaders’ interest towards the usage of the cloud. False practice may cause information security accidents or disasters (Balanagalakshmi, D. B., Bullard, D., and Kumar, S. 2020) [20]. At last, the involvement of third parties may lead to increased vulnerability to cyber-attacks and cyber-crimes. If a cyber-attack effectively destroys its system, causing consumer data loss and equipment interruption, it will be a fatal attack on the image of the virtual bank. In other words, it is extremely vital to enhance the security in virtual banks.

Modern risk management methods should be implemented for new risks discovered. Closer cross-border cooperation with Asian financial technology centers is the first step in promoting risk management of financial technology (such as virtual banks) in Hong Kong. Since 2017, the HKMA [21] has signed several cooperation agreements with mainland China and other countries to jointly establish a cross-border infrastructure based on distributed ledger technology to digitize and exchange trade documents between the two cities to minimize fraud and increase productivity.

Legal means are the other form of risk control. However, in different jurisdictions, the legal basis for liability will vary. Therefore, one possible option is to compromise the choice of jurisdiction through an arbitration clause to prevent confusion. Therefore, the information risks of virtual banks mainly exist in data privacy, data transmission, and third-party participation. There are no specific technical measures to solve these problems, but to prevent risks, the relevant institutions and scholars have studied and formulated a series of management regulations to maintain the business sustainability of the organization.

3.6. Hong Kong's Regulations on Virtual Banks

Hong Kong's Regulations on Virtual Banks was primarily enacted by the Hong Kong Monetary Authority (HKMA), which heightens the security level of virtual banks in Hong Kong, providing new experiences for bank customers, and helping retain its business sustainability. In order to promote the introduction of virtual banks, HKMA released a revised version of the Guidelines on the Authorization of Virtual Banks on 30 May 2018 [21], interpreting the HKMA's licensing principles from multiple dimensions such as funding requirements, risk management, and business plans.

The 14th and 15th guidelines have provisions on the IT risk of virtual banks, which states that "Technology related risk, especially information security, system service sustainability and BCM, is of vital importance to a virtual bank." (HKMA, 2018) [21] Additionally, the HKMA requires that "A virtual bank applicant is required to commission a qualified and independent expert to perform an independent assessment of the adequacy of its planned IT governance and systems and to require it to review it regularly." The regulations does not elaborate on specific IT risk management requirements, but only require that it should be "fit for purpose". Therefore, judging the main risks of virtual banks and their management measures is based on the differences in the main customers they serve, or in other words, their risk management is also customer oriented.

Furthermore, the business operation of virtual banks in Hong Kong must follow the Code of Banking Practice issued by the Hong Kong Association of Banks (HKAB). In terms of customer data acquisition, use, and storage, they must comply with the Personal Data (Privacy) Ordinance (the "PDPO"). From the aspect of data protection, "PDPO" stipulates that data users are required to take all practical steps to protect personal data from unauthorized or accidental access, processing, deletion, loss, or use (PCPD, HK, 2008) [22].

As a result, the virtual banks must adopt contractual specifications or other methods (such as BCM) to ensure that data processing meets data security requirements and to maintain its business sustainability.

3.7. Mainland China Regulations on Virtual Banks

Due to the close connection area of Hong Kong being Mainland China, many Hong Kong virtual bank users may live in Mainland China, and the cross-border customer virtual bank services must comply with the concerned laws and regulations in Mainland China, we also studied some regulations and laws on virtual banks in Mainland China, which will also alleviate the concerns and anxiety of virtual banks users about security risks and thereby maintaining business sustainability.

There is no specific definition of virtual banks in Mainland China, but analogically, there are some functionally similar bank services such as online banking services and electronic banking services in Mainland China. They all should abide by the same regulations

as normal banks. As we can see from the full text of that regulations in China Banking and Insurance Regulatory Commission (2020) [23], to protect and prevent the risk in bank services, in 2011, the China Banking Regulatory Commission issued the “Guidelines for the Supervision of Business Continuity of Commercial Banks”. Those guidelines are China’s first official regulatory requirement in banks’ BCM, which made more systematic provisions for BCM of the banks in China, and mentioned that commercial banks should determine appropriate BCM strategies based on their overall basic risk control strategies and risk preferences, effectively fulfill social responsibilities, protect the legitimate rights and interests of customers, and maintain financial order and its business sustainability. When business interruption events occur, the commercial banks should disclose information in a timely and accurate manner as well (Baidu Wenku, 2018) [23].

Apart from that, in general, the virtual banks are Internet applications and products, so they also have to follow some relevant laws in Mainland China, such as The Cybersecurity Law of the People’s Republic of China. As mentioned in the contents of that law provided by Baidu baike (2016) [24], if the providers of Internet products and services want to collect their customers’ information, they shall clarify it to the users and obtain their consent. They must also assure customers that their information is under near-perfect safe protection. Once the information safety incidences happen, remedial actions should be taken promptly, and related customers should be informed at once (Baidu baike, 2016) [24].

4. Survey Results and Analysis

4.1. Survey Background

As the risks that virtual banks may face in customers’ information security, we investigated the potential problems of virtual banks in the face of disasters and conducted quantitative analysis, which gives the qualitative analysis a social and realistic foundation. On this basis, we found that virtual bank customers tend to use BCM plans more for risk prevention and control, and the IT risks will do harm to the banking business sustainability.

4.2. Data Analysis Method Selection

After the basic comprehension of BCM and the recognition of the risks and the anxieties that the users may face in using the virtual banks, we should find the relationships between the identified risky factors and Hong Kong’s virtual bank users’ understanding in using BCM or the attitude toward applying BCM. Hence, it is crucial to understand how Hong Kong residents would most likely to deal with these issues after a disaster, because it can to some extent prevent residents from losing trust in virtual banks, thus maintaining the banking business sustainability and reducing the risks brought by the disaster.

Based on the above arguments, in this study, the questionnaires were used to study Hong Kong residents. One of the questions set in this questionnaire asks people to choose the disaster recovery measure they most prefer from one of four options: (A.) enhance the management and review of the information system security; (B.) use BCM to treat the emergency; (C.) raise the emergency management awareness of virtual bank employees; (D.) other methods you want. We assume that if the respondents choose BCM as a post-disaster reconstruction measure, this variable is 1 and otherwise 0. That is, we regard it as a binary attribute.

In view of the affirmed attribute type, we may review some predictive and inferential statistics methods which utilize the obtained data to make predictions, forecasts, and estimates to assist in relationship discovery. Since the aim is to estimate the accuracy of the classified group according to the target attribute type, we can use some elementary methods based on classification, such as logistic regression, the support vector machine, k nearest-neighbor, random forest, and the decision tree. Each classification method has its own advantages and disadvantages in terms of speed, memory and flexibility. Since our problem is of binary classification type, logistic regression (LR) is the best candidate classification tool in our research.

To support our choice of classification tool, Daniel Jurafsky and James H. Martin (2009) [25] proposed that not only is LR extraordinarily fitted to figure out the connections or cues between the given outcomes and some special features, but also it performs the binary decision extremely well. Moreover, some of the previous published studies have also applied LR in analyzing the bank's risk factors and the related topics, such as the examples shown in Table 1, the bank's reliability calculation (Ravi, V., and Madhav, V., 2021) [26], the estimate of the bank risks (Breed, D. G et al., 2019) [27], the evaluation of the consumers' credit risk (Abid, L et al., 2018) [28], the assessment of the natural risk factors (Davis, L., and Harden, C., 2014) [29], and the prediction of the risk indexes for the banking failure (Taha Zaghdoudi, 2013) [30].

Table 1. Previous studies.

Study	Research Aim	Main Data Analysis Method	Study Type
(Ravi, V., and Madhav, V., 2021) [26]	The calculation of the reliability and robustness of Spanish banks, Turkish banks, and UK banks.	LR model, Particle Swarm Optimization	Empirical
(Breed, D. G et al., 2019) [27]	The estimate of the banking risk and loss according to the IFRS 9	Weighted LR model	Empirical
(Abid, L et al., 2018) [28]	The evaluation of the consumers' risk on the credit in Tunisian commercial bank	LR model, discriminant analysis	Empirical
(Davis, L., and Harden, C., 2014) [29]	The assessment of the fluvial risk factors affecting the bank stability in West Tennessee (USA)	LR model	Empirical
(Taha Zaghdoudi, 2013) [30]	The prediction of the risk indexes for the failure of the Tunisian banks	LR model	Empirical
(Chen, F et al., 2020) [31]	The analysis of the risks of the windshear at Hong Kong International Airport (HKIA)	LR model	Empirical
(Harris, C., 2018) [32]	The evaluation of the risk factors caused by the invasive non-native plants to the local ecosystem	LR model, Random Forest model	Empirical
(Facile, I et al., 2021) [33]	The estimate of the risk elements to the anastomosis in the surgery recovery	LR model	Empirical
(Cuadrado-Godia, E et al., 2019) [34]	The calculation of the ranking of stroke and cardiovascular risk factors	LR model	Empirical
(Fügener, S et al., 2015) [35]	The identification of the risk factors in Fracture-Healing	LR model	Empirical

Apart from that, many researchers have utilized LR in the analysis of risk factors in other areas, such as the fields of weather and climate. Chen et al. (2020) [31] used LR to analyze the risks of the windshear at Hong Kong International Airport (HKIA). In the ecological environment area, Harris (2018) [32] pointed out that LR was able to figure out the risk factors caused by the invasive non-native plants to the local ecosystem. In terms of human health, Facile et al. (2021) [33], Cuadrado-Godia et al. (2021) [34], and Fügener et al. (2021) [35] have mentioned that LR could be applied in the aspect of disease treatment, disease recovery, and surgical results in analyzing the risk determinants.

In summary, the LR model matches our study topic and the requirement of the data processing; we chose it as our data analysis means for the study group.

In addition, before the LR analysis, we should conduct some descriptive statistical analysis on the obtained data to find out its characteristics and whether it is representative of Hong Kong's virtual bank users.

4.3. Descriptive Statistical Analysis

The data used in this study were obtained from the questionnaire surveys, and the respondents were mostly Hong Kong residents. We used social media method to invite friends from special interest groups and university students as our target respondents. Such respondents are from all walks of life and they can be representatives of the whole research population. A total of 280 valid samples were collected and validated after filtering out the invalid questionnaires. The descriptive statistical analysis of the samples is shown in Table 2.

Table 2. Descriptive statistical analysis results.

Question	Content	Number	Proportion
Age	Under 18 years old	10	3.57%
	18–25 years old	180	64.29%
	26–30 years old	60	21.43%
	31–40 years old	30	10.71%
Monthly Income	Less than 10,000 HKD	110	39.29%
	10,000–20,000 HKD	80	28.57%
	20,000–30,000 HKD	50	17.86%
	More than 30,000 HKD	40	14.29%
Education Level	High school or below	10	3.57%
	Bachelor's	80	28.57%
	Master's degree or above	180	64.29%
Monthly Usage of VB	Less than one	60	21.43%
	One to three times	90	32.14%
	Three to ten times	60	21.43%
	More than ten times	70	25.00%

(1) Analysis on the question item “Age”

According to the analysis results of the related question item “Age” in Table 1, we can find that majority of the respondents in our questionnaire surveys are under 25 years old, which means the sample gears towards young people. At the same time, as per Sing Tao Daily's news about the customers' information of the Airstar Bank [36], one of the virtual banks approved by the HKMA in the earliest period, most of Airstar Bank's customers are aged between 20 to 40, thus this bank's customer age trend is also young. Similarly, according to the information by ZA Bank [37], the No.1 virtual bank in Hong Kong, many individuals born post-90s have become the ZA Bank's customers and have become insured.

As a result, from the “Age” dimension in the question items, the study sample can comparatively represent the most of the virtual bank users in Hong Kong.

(2) Analysis on the question item “Monthly Income”

From the results of question item “Monthly Income” in Table 1, we are aware that in the study group, the proportion of the number of classified groups gradually falls with the increase in monthly income, which reflects the general society laws; that is, the number of those with low income is high while the number of those with high income is low.

(3) Analysis on the question item “Education Level”

As we can see from the results about question item “Education Level” in Table 1, we noticed that most of the respondents in the study group have an advanced education background with a master's degree or above, the others in the study group have obtained their bachelor's, and few of them have an education background in high school or below. Meanwhile, a homologous result is also displayed in the news relevant to the Airstar

Bank's customer information by Sing Tao Daily [36]; 77% of the bank's customers have an education background at post-secondary/university level or above.

Hence, the result of the "Education Level" dimension in the question items shows that the study sample has a certain degree of representativeness among Hong Kong's virtual bank users.

(4) Analysis on the question item "Monthly Usage of VB"

It can be seen from the results of the question item "Monthly Usage of VB" in Table 1 that 21.43% of the people in the study group use virtual banks less than once a month, and the frequencies with which others use virtual banks can be seen as evenly distributed. The individuals' frequency in using VB in the sample may demonstrate that for virtual banks, different people have different usage needs and habits.

Generally speaking, on account of the analysis results in Table 2, the sample mainly contains young people with advanced education whose monthly income is higher than the average (except for students without jobs), and most of the respondents have used or known about VB. Therefore, they are relatively representative for the entire population of Hong Kong's virtual bank customers and are able to provide reference value for our study.

4.4. LR Analysis

After the data analysis method selection and the classification and summary of the questionnaire results, we conducted a LR with the target variable (i.e., BCM) as the dependent variable, so as to explore and analyze the factors affecting people's expectation of using BCM as a post-disaster solution. All variables in LR were derived from questionnaires. These variables include whether Hong Kong residents have been exposed to disasters or risks, how often they use virtual banks, and what they expect to do after a disaster, and so on. The meanings and results of all the variables can be found in Table 3. SPSS was used for LR analysis handling 280 data resources collected.

As can be seen in the regression results, "dataRisks" is significant in the 95% confidence interval, and LR coefficients were 25.019, suggesting that compared with other residents of Hong Kong, people who think virtual banks have data risks are 24 times more willing to use BCM as a post-disaster solution. "dataBreaches", "choiceAfterDisaster", and "frequency_1-3" are not significant, so these three factors will not be discussed in this study. People who have encountered a fake bank website or think disasters have impacts on VB are more willing to apply BCM, which is in line with expectations. In addition, the higher the frequency of using virtual banks, the higher the recognition of BCM. Above all, those who expect the virtual bank to be running in less than ten minutes are most likely to apply BCM.

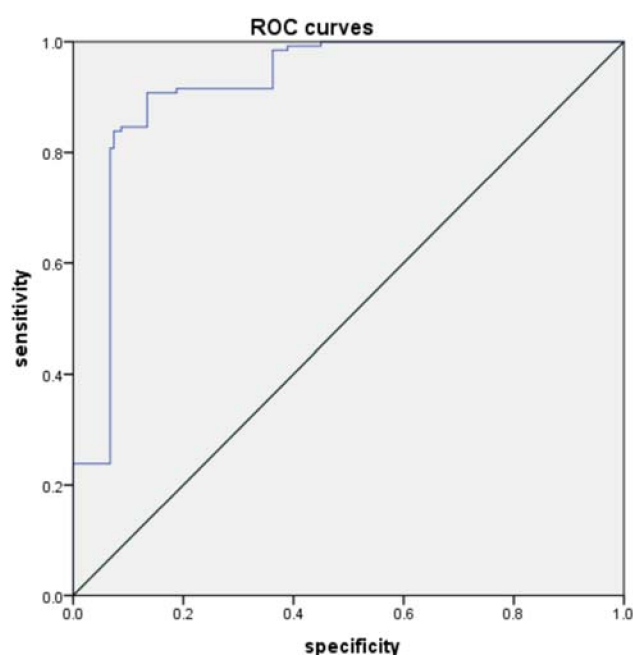
The above analysis results indicate that the customers of virtual banks who are valued most, such as those who frequently use virtual banks or want to resume business as soon as possible, are more likely to agree to use BCM as a post-disaster solution.

To further verify the accuracy of the LR model, the receiver operator characteristics curve (ROC curve) analysis was carried out in SPSS. With "1-specificity" as the x-coordinate and sensitivity as the y-coordinate, the accuracy of the evaluation results of the dependent variable can be compared. The ROC curve method reflects and compares the accuracy of model evaluation and prediction through the area under the ROC curve (area under curve, AUC). When the AUC value is above 0.9, the evaluation accuracy of the model is particularly good. As shown in Figure 2, the AUC values of all the data of the LR model are 0.918, which has a high prediction accuracy. The AUC values further indicate that the LR model has a good prediction performance and application value in the prediction of the public's recognition of BCM. Therefore, this LR model can be used for BCM recognition evaluation.

Table 3. LR analysis results.

Variable Name	Meaning	B	df	Significance	Exp (B)
dataBreaches	Whether have ever experienced a data breach	20.715	1	0.998	9.9×10^8
fakeBankWebsite	Whether have encountered a fake bank website (such as a phishing website)	2.244	1	0.004	9.429
dataRisks	whether think virtual banks have data risks	3.220	1	0.000	25.019
disasterImpactOnVB	Whether think disasters have impacts on VB	0.265	1	0.032	1.304
choiceAfterDisaster	Whether choose this VB after a disaster	−18.455	1	0.999	0.000
frequency_1–3	Use the virtual bank 1–3 times a week	−0.024	1	0.960	0.976
frequency_3–10	Use the virtual bank 3–10 times a week	1.349	1	0.023	3.853
frequency_above10	Use the VB more than 10 times a week	1.432	1	0.010	4.185
recovery_1hour	Expect to resume business within 1 h	0.017	1	0.000	1.017
recovery_10minutes	Expect to resume business within 10 min	0.051	1	0.000	1.052
instants	Instants	0.218	1	0.761	1.244

Note: “B” represents LR coefficient, which represents the impact of each evaluation factor on the risk; “df” is degrees of freedom.

**Figure 2.** Subject characteristic curve.

4.5. Risk Analysis of Virtual Bank

Virtual banks in the 21st century are becoming an important means for financial institutions to broaden their service areas, achieve business growth, adjust business strategies, and promote financial development. At the same time, since its merger has the dual characteristics of the banking industry and modern information technology, the development of virtual banking has brought a series of new risks based on the general risks of the traditional banking industry, which poses greater challenges to the sustainable development and risk prevention of the banking industry. Hence, we also analyzed the risks that virtual banks may face through our survey study.

In Figure 3, the results show that most people consider virtual banks to be extremely risky. In order to alleviate the concerns of consumers, risk prevention and control of virtual banks are essential. Then, we investigated the types of virtual bank risks. In Figure 4, among the risks, IT risk accounts for 78% of all risks, such as information and data leakage,

network default, phishing sites, etc., thus we can focus on how to solve the problem of prevention and control of IT risks.

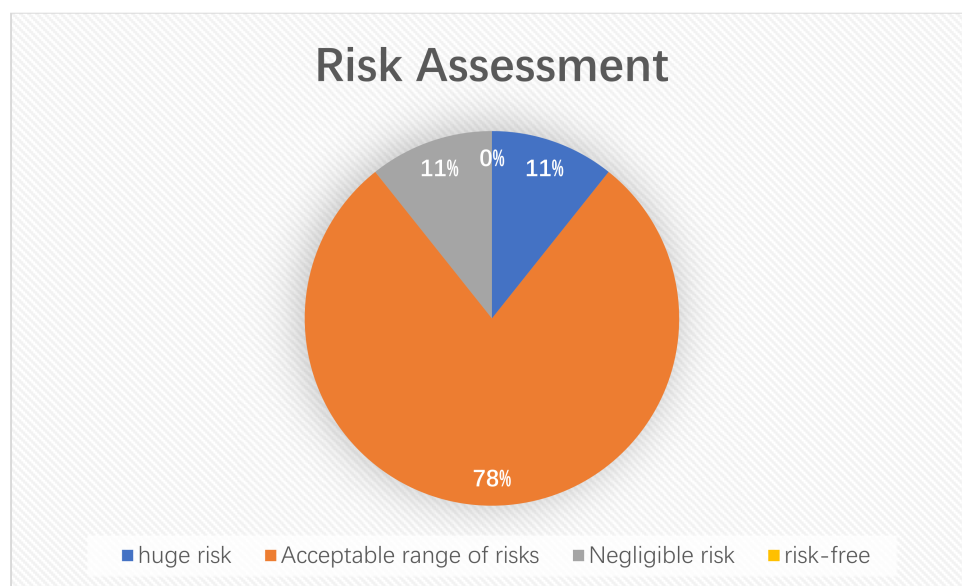


Figure 3. Risk assessment.

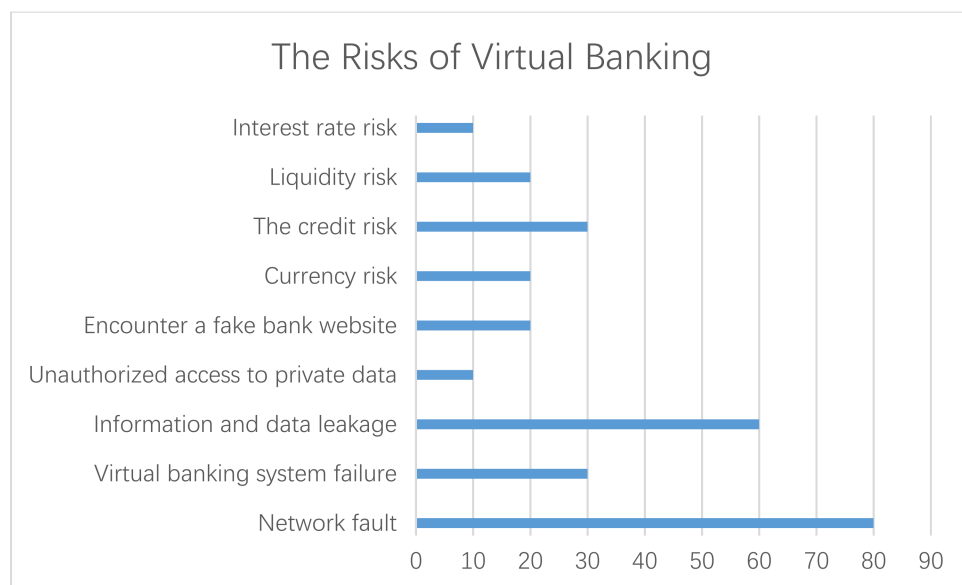


Figure 4. The risk of virtual banking.

4.6. Business Ranking Analysis


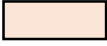




To figure out which businesses we should rescue first in the event of a disruption, we surveyed people about the importance of virtual banking in their minds. First, we ranked the importance of virtual banking services, and the statistical results are shown in Table 4 below.

Table 4. Importance ranking of virtual banking services.

Business Name	Importance Ranking					
	First	Second	Third	Fourth	Fifth	Sixth
Core Business System	110	50	20	20	40	40
Electronic Payment System	90	100	30	30	20	10
Electronic Account System	0	90	110	30	40	10
Mobile Banking Service	40	30	70	80	60	0
Personal E-bank	30	10	40	10	80	20
Financial Management System	10	0	10	20	40	200

We then weighted each business option to calculate the average ranking. Finally, the final ranking is represented by Table 5. As can be seen from the figure, the payment system is the most important, followed by the core business system, and the third is the electronic account system. Therefore, we should first consider restoring these important businesses in the hearts of customers when developing the BCM strategy to mitigate the impact of business disruption on the operational service and the business sustainability of virtual banks.

Table 5. Final ranking of business importance.

System Name	Average Ranking	Final Ranking
electronic payment system	 2.36	1
core business system	 2.82	2
electronic account system	 3.18	3
mobile banking	 3.32	4
personal e-bank	 3.89	5
financial management system	 5.43	6

4.7. IT Disaster Recovery Analysis

BCM encompasses IT disaster recovery and increases a virtual bank's resilience to business interruptions and minimizes the impact of such interruptions, which can keep the banking business sustainable. To make IT disaster recovery plan more effective, we measured consumer demand for recovery time after a disaster. The data in Figure 5 shows that 46% of consumers chose within 10 min, 25% of consumers chose within one hour, and the rest of them choose within one day. In general, the shorter the recovery time, the less losses will be incurred and the better the outcome for the virtual bank.

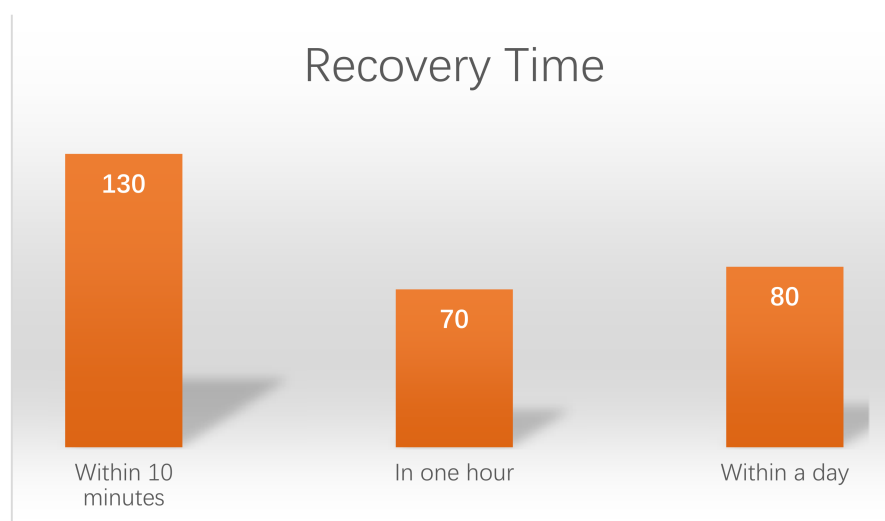


Figure 5. IT Disaster Recovery Time.

Finally, we investigate whether consumers would choose virtual banks again after the disaster. According to the data in Figure 6, about half of them refused to use virtual banks again. This shows that the disaster had a high adverse impact on the reputation of virtual banks and was harmful to customers' loyalty as well as the business sustainability of the virtual bank.

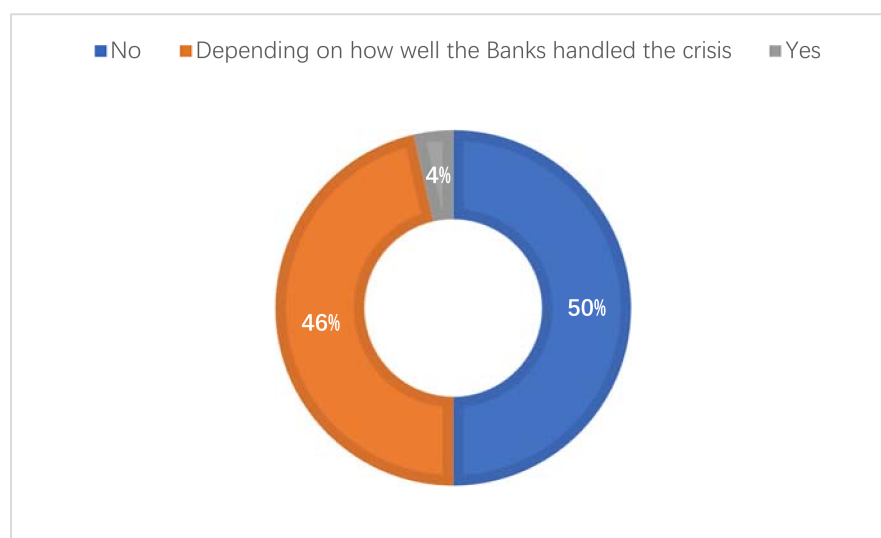


Figure 6. Consumer Choice.

As financial institutions pay increased attention to the business sustainability and the construction of BCM in order to make BCM more suitable for virtual banks in the future, our study will further explore and analyze the best practices of daily operations with qualitative methods.

5. Discussions and Case Study

5.1. The Background of the Cases Study Discussions

In accordance with the quantitative analysis, we found that the preference of the virtual bank users who often use virtual banks or consider that there are lots of risks in VB is to use BCM to safeguard their security and to evade the IT risks. Meanwhile, IT risks today are increasingly common, which debases the banking business sustainability; therefore, they are the burning issues that we should solve.

Therefore, due to the fact that we have almost no practical experiences in operating and managing virtual banks, in order to address the above customers' concerns in using virtual bank, we have conducted our qualitative analysis by researching some successful cases or relative practice in the field of virtual banks. Through studying these outstanding cases in the area of virtual banks, we are able to give some concrete suggestions to virtual banks on the implementation of BCM to maintain their business sustainability.

5.2. The Purpose of the Cases Study Discussions

The first case study is about WeBank, which is an Internet bank (virtual bank) in Mainland China, and the case study is an example of empirical research on the application of BCM in virtual banks. This case study is from the perspective of the virtual bank itself, narrating the application of BCM in virtual banks to maintain its business sustainability.

The second case study is related to MAS (Monetary Authority of Singapore), which is the central bank and the comprehensive financial regulator of Singapore. As mentioned before, some official regulators have issued many regulations, ordinances, and guidelines that claim that in virtual banks, the protection of the information security and business sustainability is a pressing need. Hence, the case study chooses the regulators as the research perspective and recounts some feasible measures of regulators in handling the troubles in the business continuity of banks to retain its business sustainability.

5.3. Case Study Discussion 1: The Illustrious WeBank

5.3.1. The Introduction of the Case Study Discussion

This case study will find some solutions for virtual banks to ensure customers' information security and virtual banks' own business sustainability via making use of BCM under the circumstances of disasters or risks. In accordance with this, WeBank performed extremely well during the COVID-19 pandemic (i.e., the massive disaster) because of the excellent application of BCM; therefore, the way to find those solutions is to analyze WeBank, which is a representative virtual bank (Internet Bank) in Mainland China. Based on the solutions, the case study will give some suggestions for virtual banks on how to guarantee business sustainability for themselves and their customers' information security.

5.3.2. A Brief Introduction of WeBank

As the information about WeBank provided by Baidu baike (2020) [38] points out, WeBank is an Internet virtual bank initiated and established by well-known private companies such as Tencent. WeBank has no additional physical and offline branches. According to the official website of WeBank (2020) [39], WeBank has strictly abided by the national financial laws, regulations, and regulatory policies, and is committed to offering near-perfect financial services to individuals and micro-enterprises in China based on compliant operation and stable development.

5.3.3. Reasons to Study WeBank

(1) WeBank is a highly representative virtual bank in Mainland China.

From the content about WeBank in Baidu baike (2020) and the official website of WeBank (2020) [40], WeBank is the first Internet bank (i.e. Virtual bank) in Mainland China, and it is a company on the Hurun New Finance Top 100 list in 2019; hence, it is highly representative.

(2) WeBank has received strong support from the policies and rules of the Chinese government.

WeBank has been strongly supported by the policies and rules of the Chinese government. For instance, as mentioned in the "About us: Milestones" part of the official website of WeBank (2020) [40], on 4 January 2015, Li Keqiang, Premier of the People's Republic of China, personally visited WeBank for investigation and research, and gave strong support to WeBank.

(3) WeBank has excellent performance in using BCM to maintain its business sustainability.

It is universally acknowledged that under the impact of the global pandemic of COVID-19 in 2020, many banks around the world have failed due to business and capital flow interruptions, while WeBank has excellent performance in the application of BCM, which is able to guarantee its own business sustainability and customers' information security. According to the news "Yao Huiya from WeBank: Fintech breaks the boundaries of banking business, opening banks help collaborative innovation" on Sohu (2020) [41] shows that since the outbreak of COVID-19, by combining its own business characteristics and making full use of the advantages of pure online business and continuous technology management, WeBank was able to ensure its own uninterrupted operation and to continue to serve small and micro enterprises and individuals in the pandemic area. Therefore, WeBank guaranteed customers' information security and its own business sustainability during the pandemic. Moreover, the article "WeBank postpones repayment for 3 months to help small and micro businesses overcome difficulties" on Sina finance (2020) [42] tells us that on 13 February, WeBank even gave timely help to customers of small and micro enterprises in distress by launching a three-month delay in repayment measures, so that they could tide over the crisis of the pandemic.

5.3.4. Solutions from Webank Case Study Discussion

(1) A shrewd governing structure is highly recommended

On the basis of the Annual Report of WeBank (2019) [43], WeBank's board of directors has five ad hoc committees, that is, the Tactic Committee, the Audit Committee, the Risk Management and Consumer Protection Committee, the Related Party Transaction Control Committee, and the Nomination and Remuneration Committee, which attach vital importance to information security and risk management. Furthermore, the Board of Supervisors is the supervisory agency of WeBank. In daily supervision, the Board of Supervisors plays a monitoring role in WeBank's strategic management, business decision-making, financial activities, risk management, internal control, and internal audit. The Board of Supervisors and its special committees strictly adhere to the codes of WeBank, deliberate and approve proposals such as comprehensive risk management reports and internal control evaluation reports each year, and effectively perform their supervisory roles.

(2) A scientific technical system architecture is necessary

From the article "The first exposure of WeBank Internet architecture" on InforQ (2015) [44], the business continuity of WeBank has reached the highest level of "GB/T 20988-2007, Information security technology—Disaster recovery specifications for information system". An example of its intuition is that each production data center of WeBank is equipped with four optical fibers that use various physical paths to access the bank's core backbone network. In other words, it is necessary to accurately cut off all the physical paths of the production data center at the same time and at different locations to make a center of WeBank lose connection, but that is almost impossible.

As mentioned from the press "Yao Huiya from WeBank: Fintech breaks the boundaries of banking business, opening banks help collaborative innovation" on Sohu (2020) [41], relying on the bank's core system based on a distributed architecture and modular design, as well as an agile organizational structure, WeBank can quickly adjust its credit strategies and product functions; it has also launched a series of effective financial relief support measures such as quickly reducing rates and fees, expanding coverage, improving quality, securing unblocked channels, and opening up green channels, in order to help small and micro enterprises and individual customers overcome difficulties. Those measures fully demonstrate the advantages of WeBank's full online product model supported by financial technology and BCM to maintain its business sustainability.

(3) Internal control strategies are required

As stated in the essay “Launched ‘We Yan Action’, WeBank consolidated compliance operations” on China Economic Net (2018) [45], in 2018, in order to handle the continuous growth of business and personnel scale, WeBank took effective measures to improve internal management and to strengthen operating infrastructure. In terms of the establishment of regulations and rules, WeBank continues to promote the normalization and standardization of various business systems, management procedures, and control methods using the principle of “internal control first, system first”, so that the bank’s rules and regulations are able to cover various major risks. This makes the security of WeBank more powerful. To further reinforcing the construction of internal control, in the same year of 2019, WeBank also continued to carry out “We Yan Action” on a whole-bank scale and conducted multiple training activities on all-round promotion of employees’ codes of behaviors. The drills covered all of the employees and outsourcing personnel. “We Yan Action” also had rounds of review and inspections on system construction and job management, and played a key role in effectively preventing risks and maintaining business sustainability.

(4) The contingency plans are significant

First of all, the business contingency plans must abide by some national or global standards. Meanwhile, for responding to interruption events and continuing or resuming activities within a predetermined time to maintain business sustainability, the contingency plans should also include some documented plans, which comprise required procedures such as the process of initiating a response to the interruption events and the consequences of handling interruption events, etc.

Secondly, the implementation of the business contingency plans must be well done. According to the essay “Yao Huiya from WeBank: Fintech breaks the boundaries of banking business, opening banks help collaborative innovation” on Sohu (2020) [41], in terms of internal operations, as an Internet bank, many employees usually need to work remotely at home, thus WeBank has deployed thousands of Virtual Desktop Interface (VDI) hosts early on, realizing the popularization of remote office tools. After the pandemic started, WeBank only needed to temporarily adjust its security policies, allowing some VDI public network access to directly support the needs of all positions for remote work at home.

Moreover, the sustainability of the plans is of vital importance as well. As per the article “Yao Huiya from WeBank: Fintech breaks the boundaries of banking business, opening banks help collaborative innovation” on Sohu (2020) [41], after the smooth resumption of work, to continue to strengthen the work of monitoring and preventing the COVID-19 and to ensure the operational sustainability, WeBank also developed and launched a health code application based on blockchain technology for internal employees to facilitate internal supervision and auditing.

5.4. Case Study Discussion 2: Benchmarking with Singapore Regulation

5.4.1. The Preamble of the Case Study Discussion

It is universally acknowledged that all banks in the world should follow the local official policies and regulations, otherwise the banks in violation of the relevant provisions will be punished or even be forbidden to continue their business, which is deleterious to their business sustainability; therefore, according to their local governmental and regulatory demands, an increased number of banks are implementing the required internal policies and external regulations, including the virtual banks. Further, some of the regulatory agencies can offer certain supervision solutions in the aspect of BCM for the banks’ sustainable development. Therefore, we also hope to gain inspiration from some governmental and regulatory agencies of virtual banks so that virtual banks are able to better apply BCM in order to maintain their business sustainability, so as to better serve society.

5.4.2. A Concise Introduction to MAS

According to the content from the official website of MAS (2019) [46], the Monetary Authority of Singapore (MAS), which is the central bank and synthetic financial regulator of Singapore, has boosted a steady national financial business in Singapore through its

prudential supervision of all financial institutions, which includes the virtual bank. MAS oversees monitoring the financial and investor markets by regulating their conducts and upgrading their skills to maintain their business sustainability. Moreover, MAS has also cooperated with the international financial industry to promote Singapore's status as a dynamic international financial center.

5.4.3. Causes for Researching Singaporean Regulation

Since the research topic is enhancing the users' information security management in the virtual banks of Hong Kong by BCM to maintain its business sustainability, we should consider some successful cases in Hong Kong or other regions similar to Hong Kong and use them as our research arguments; therefore, Singapore is a wonderful selection. Due to the following similarities between Hong Kong and Singapore, we can standardize the BCM principles for virtual banking business via the IT risk management requirements of the Singapore Monetary Authority.

(1) The analogous market scales

As announced in the official websites of HKMA (2020) [47], there are currently eight officially licensed virtual banks in Hong Kong, and six of them have been opened, but because people may not be used to them, their business statutes are not particularly good. In the meantime, according to the content provided by MAS (2020) [48], the opening applications of fourteen companies have been initially approved and the virtual bank market is expected to be similar in size to Hong Kong. In general, both Hong Kong and Singapore are in the beginning of the market of the virtual banks business.

(2) The alike economic standing

It can be seen from the content of Hong Kong and Singapore in Baidu baike (2020) [49,50] that London, New York, and Hong Kong are three of the most distinguished international finance centers in the world, and in 2018, Singapore became the fourth largest international financial center. Therefore, in the world, the economic standing of Singapore is commensurately close to that of Hong Kong.

(3) The allied population scopes

As we know, the population is a critical indicator to measure the market vigor of virtual banks. In the information of Hong Kong provided by Baidu baike (2020) [49], at the end of 2019, there were nearly 7.52 million people settled in Hong Kong. From the Baidu baike (2020) [46] of Singapore, in the same year, Singapore had about 5.7 million residents, which is close to the population of Hong Kong.

(4) The similar land area

The land area is also a vital index to judge the market size of the virtual banks. In accordance with the information of Hong Kong and Singapore in Baidu baike (2020) [49,50], Hong Kong covers an area of approximately 1106.66 square kilometers, which is about the same as Singapore's 724.4 square kilometers.

5.4.4. Inspirations from MAS Case Study Discussion

(1) Internal risk prevention and control organization are necessary

MAS (2013) [51] requests that "For the sake of the handy and swift detection of the adverse and malicious activities from the internal and the external, it is obligatory for the banks to set up some adequate secure monitoring organizations and working procedures." Generally speaking, the risk prevention and control organization under the board of directors is the BCM organization with the highest authority and is responsible for the company's overall risk prevention and control and business sustainability operations. At the implementation level, the risk prevention and control organization need to include specific departments, such as IT, business department, internal control, legal, and other departments. Those departments implement internal risk prevention and control matters, business linkage plans, and business sustainable operations by improving policies and specific tasks.

As per the recommendations of MAS, the virtual banks ought to prompt the capabilities of dealing with financial losses and to build the functions of the emergency analysis and the pressure testing for better evaluating the effect of environmental risks on the circumstances of their risks and their business sustainability (MAS, 2020) [52]. Considering the uncertainties of environmental changes and long-term prospects, these scenarios should be combined with forward-looking forecasts and information as a supplement to historical data, because the latter may systematically underestimate potential risks.

(2) The importance of IT risk prevention and recovery plan

As suggested by MAS (2013) [51], “A technology risk management framework should be established to manage technology risks in a systematic and consistent manner.” The Monetary Authority of Singapore has proposed an IT risk prevention and control framework for ensuring the banks’ business sustainability. The first step is to clarify the roles and responsibilities of IT risk management, the second is to analyze the value of the system, the third is to evaluate the possibility of risk, the fourth is to analyze and implement appropriate prevention and BCM methods, and the fifth is the need for periodic report, monitor, and review. The organizational guarantee mentioned in the first point is particularly important.

At the same time, the requirements for disaster recovery plans were also put forward. In order to heighten recovery measures related to large-scale interruptions and achieve risk diversification, banks should deploy fast backup and recovery functions at the level of individual systems or application clusters. Banks should consider the interdependence among key systems when developing recovery plans and conducting contingency tests and verify the effectiveness of recovery requirements at least annually. The recovery site should be separated from the main site so that critical systems and business operations can be restored and remain sustainably operational in the event of an outage at the main site.

6. Recommendations for Virtual Banks

From the above analyses and findings, this article summarizes three management recommendations on strengthening the security management of customer information in the virtual banks of Hong Kong through BCM to maintain its business sustainability.

(1) Build overall BCM blueprint

To radically simplify management, improve efficiency, and ensure the sustainability of banking business, the virtual bank needs to clarify the institution responsible for BCM and the overall BCM blueprint in accordance with the external regulatory requirements, the company’s business development principles, and the business prioritization. First, the virtual bank needs to form a BCM committee; generally speaking, they are the board of directors, responsible for sustainable corporate continuity management and taking the lead in drawing up the overall blueprint. Further, the blueprint should include general principles, basic standards, and specific procedures, such as emergency guidelines, related emergency responsibilities, emergency actions, and so on. At the same time, according to the specific types of safety accidents, hazards and emergency support, the blueprint should clearly guide emergency participants to perform quick recovery actions. After the blueprint is completed, the related departments need to conduct business analysis, risk assessment, and establish a long-term evaluation mechanism. After establishing the BCM blueprint system, the virtual bank shall manage and maintain the disaster recovery plan and make timely revisions.

(2) Establish BCM management teams based on risk assessment

In the application of BCM, apart from the BCM committee, a virtual bank should have some BCM management teams under the BCM committee to take charge of some detailed affairs. The suggested BCM management teams should abide by some of the VB’s inner codes and would be responsible for handling information risk, operational risk, and technology risk in the fields of banking infrastructure, daily operations, customer services, payment services, and loans services to ensure the business sustainability by using the methods of compliance and legislation, so that the VB is able to relieve users’ anxiety regarding IT risks. Moreover, to cover the above requirements, the BCM management

teams of the VB should be in three tiers. The top tier is the strategic management team, which is a strategic team to address firm-scale accidents, to formulate the inner control strategies, and to frame a scientific technical and physical system architecture for the VB. The second tier is the operation crisis management team, which is a team to address functional practice incidents that will almost be solved by predetermined plans, namely contingency or recovery plans. Additionally, the third tier is the incident management team, which is a team to address office-level incidents such as individual office computers breaking down, etc.

(3) Improve IT disaster recovery plan of core systems

Due to the strong dependence of virtual banks on IT systems, virtual banks must formulate and continuously optimize IT disaster recovery plans for key systems (such as the payment systems and the core business systems) to minimize the impact of emergencies on the business and to enhance the ability of the bank sustainable development. The recovery plan is established to identify critical IT assets and prioritize their recovery needs, including reactions, recovery procedures, logging, and documentation throughout the IT process. Generally speaking, an IT disaster recovery plan, needs to be prepared by the technical team and the BCM coordinator and approved by the BCM committee. Specifically, it is first necessary to conduct a risk assessment of the company's key business systems, sort the different risks of the key systems, and clarify the scope and objects of the recovery plan. Moreover, the arrangement of the IT disaster recovery plans for the virtual banks should also consider the crisis response and urgent contact plans for the whole groups of the stakeholders to further ensure its business sustainability.

In summary, in order to strengthen the security management of customer information in the virtual banks of Hong Kong through BCM to maintain its business sustainability, virtual banks can take the following measures. First, a complete blueprint for BCM is required to achieve top-down overall management; second, in response to different key risks, it is necessary to establish an executive-level BCM management team to be specifically responsible for and implement risk assessment, policy formulation, inspection and review, etc. Third, due to the strong dependence of virtual banks on IT systems, they need to focus on key points of the information system of the bank, which needs to improve the IT disaster recovery plan.

7. Conclusions

The purpose of this research is to find out how to use BCM for Hong Kong's virtual banks when trying to reduce customer information risks so as to maintain its business sustainability.

From our data analyses, we found that consumers would be highly concerned about the reliability of the services provided by virtual banks and that financial institutions would pay more attention to business sustainability. These are of paramount importance to the virtual banks' critical success factor. Through the two case studies, the nature of the problems affecting virtual banks' business continuity has been dug out. Based on those findings, three recommendations for strengthening virtual banks' security management through BCM were derived.

The main limitation of this research is lack of funding to conduct a large-scale survey study to improve the reliability of data analyses. We hope that this research article can arouse the attention of authorities and grant us some funding for further elaborating the survey study and more in-depth detail case studies through action research methodology.

Author Contributions: Conceptualization, H.C. and P.S.; methodology, H.C. and P.S.; data analysis software, G.G.; validation, C.Y. and G.G.; data analysis, H.C., C.Y. and G.G.; investigation, G.G.; data curation and collection, C.Y. and G.G.; writing—original draft preparation, H.C., P.S., G.G. and C.Y.; writing—review and editing, D.T. and H.C.; visualization, G.G.; supervision, D.T.; project administration, D.T. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Institutional Review Board Statement: Ethical review and approval were waived for this study, due to the fact we conducted the questionnaire survey in Hong Kong and strictly abided by the Personal Data (Privacy) Ordinance (PCPD) in the Data Privacy Law of HKSAR through making a declamation at the start of our questionnaire survey, which is ‘This survey is an anonymous survey, only for our research study this time, you are not compulsory to participate in this survey. This questionnaire survey research is entirely dependent on your voluntary help, and all your information will be kept strictly confidential and will be cleared after the survey. If you can take a few minutes to participate in this survey, we would be very grateful!’

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

Acknowledgments: We thankfully acknowledge the wenjuan.com powered by Shanghai Zhongyan Network Technology Co., Ltd. for providing the questionnaire survey service and the WeChat powered by Tencent Technology (Shenzhen) Co., Ltd. for providing the customer groups for questionnaire investigation. We also appreciate the constructive suggestions and comments from the editor and reviewers.

Conflicts of Interest: The authors declare no conflict of interest.

References

- Bojanc, R.; Jerman-Blažič, B. A Quantitative Model for Information-Security Risk Management. *Eng. Manag. J.* **2013**, *25*, 25–37. [CrossRef]
- Ahmadalinejad, M.; Mohsen Hashemi, S. A National Model to Supervise on Virtual Banking Systems through the Bank 2.0 Approach. *Adv. Comput. Sci. Int. J.* **2015**, *4*, 83–93.
- Qu, X. Research on business Continuity Oriented Guangdong Huaxing Bank’s Information System Disaster Recovery Management Optimization. Master’s Thesis, Lanzhou University, Lanzhou, China, 2020.
- VirtualBank, a Division of First Horizon Bank. About Us. 2021. Available online: <https://www.virtualbank.com/about-us/> (accessed on 21 September 2021).
- IFEC. What is a Virtual Bank? 2020. Available online: <https://www.ifec.org.hk/web/en/financial-products/fintech/virtual-bank/what-is-a-virtual-bank.page> (accessed on 10 October 2020).
- Hong Kong Monetary Authority (HKMA). Guideline on Authorisation of Virtual Banks. 2000. Available online: <https://www.hkma.gov.hk/eng/news-and-media/press-releases/2000/05/20000505-3/> (accessed on 21 September 2020).
- Hong Kong Monetary Authority (HKMA). Press Releases. 2019. Available online: <https://www.hkma.gov.hk/eng/news-and-media/press-releases/virtual-banks> (accessed on 21 September 2020).
- Ma, W. Research on Financial Business Continuity Management System. *Leg. Econ.* **2014**, *10*, 110–111.
- Aboobucker, I.; Bao, Y. What obstruct customer acceptance of internet banking? Security and privacy, risk, trust and website usability and the role of moderators. *J. High Technol. Manag. Res.* **2018**, *29*, 109–123. [CrossRef]
- Li, F.; Lu, H.; Hou, M.; Cui, K.; Darbandi, M. Customer satisfaction with bank services: The role of cloud services, security, e-learning and service quality. *Technol. Soc.* **2021**, *64*, 101487. [CrossRef]
- Conger, S. The impact of the COVID-19 pandemic on information systems management. *Inf. Syst. Manag.* **2020**, *37*, 327–331. [CrossRef]
- Muparadzi, T.; Rodze, L. Business Continuity Management in a Time of Crisis: Emerging Trends for Commercial Banks in Zimbabwe during and Post the COVID-19 Global Crisis. *Open J. Bus. Manag.* **2021**, *9*, 1169–1197. [CrossRef]
- Sohu. The First Bank in the United States Has Closed Down Since the Outbreak of the Epidemic! There Were also Bank Failures in China, and Three Cases Were Not Compensated. 2020. Available online: https://www.sohu.com/a/385833051_120510170 (accessed on 30 October 2020).
- Miao, M.; Saide, S.; Ratna, S.; Muflih, M. Business Continuity Innovation in Disruption Time: Sociotechnical Systems, Business Analytics, Virtual Business, and Mediating Role of Knowledge Absorptive Capacity. *IEEE Trans. Eng. Manag.* **2021**, *30*, 1–12. [CrossRef]
- Zhang, X.; Han, S.; Xie, Z. Introduction to related standards of Business Continuity Management System (BCMS). *China Qual. Stand. Rev.* **2019**, *2019*, 14–16.
- Baidu Baike. Business Continuity Management. 2020. Available online: <https://baike.baidu.com/item/%E4%B8%9A%E5%8A%A1%E8%BF%9E%E7%BB%AD%E6%80%A7%E7%AE%A1%E7%90%86/6812815?fr=aladdin> (accessed on 14 October 2020).
- Hong Kong Monetary Authority (HKMA). HKMA Introduces Key Measures on Sustainable Banking and Green Finance. 2019. Available online: <https://www.hkma.gov.hk/eng/news-and-media/press-releases/2019/05/20190507-4/> (accessed on 3 August 2021).
- Li, G. Lay a solid institutional foundation for the sustainable development of non-contact banks. *China Bank* **2020**, *2020*, 35–37.

19. Bryan Cave Leighton Paisner. Virtual Banks in Hong Kong: Bringing Risks and Opportunities to Asia. 2018. Available online: <https://www.bclplaw.com/en-GB/insights/virtual-banks-in-hong-kong-bringing-risks-and-opportunities-to.html> (accessed on 10 October 2020).
20. Balanagalakshmi, D.B.; Bullard, D.; Kumar, S. Cloud Computing Technology-Security Issues in Banks-An Overview. *Eur. J. Mol. Clin. Med.* **2020**, *7*, 5299–5304.
21. Hong Kong Monetary Authority (HKMA). BANKING ORDINANCE Authorization of Virtual Banks A Guideline Issued by the Monetary Authority under Section 16. 2018. Available online: <https://www.hkma.gov.hk/media/eng/doc/key-information/press-release/2018/20180530e3a2.pdf> (accessed on 14 October 2020).
22. Office of the Privacy Commissioner for Personal Data, Hong Kong (PCPD). Personal Data (Privacy) Ordinance (Cap. 486). 2021. Available online: https://www.pcpd.org.hk/english/data_privacy_law/ordinance_at_a_Glance/ordinance.html (accessed on 14 October 2020).
23. China Banking and Insurance Regulatory Commission. Guidelines for the Supervision of Business Continuity of Commercial Banks. 2020. Available online: <http://www.cbirc.gov.cn/cn/view/pages/ItemDetail.html?docId=909385&itemId=4115&generalType=9> (accessed on 14 October 2020).
24. Baidu baike. The Cybersecurity Law of the People's Republic of China. 2020. Available online: <https://baike.baidu.com/item/%E4%B8%AD%E5%8D%8E%E4%BA%BA%E6%B0%91%E5%85%B1%E5%92%8C%E5%9B%BD%E7%BD%91%E7%BB%9C%E5%AE%89%E5%85%A8%E6%B3%95/16843044?fr=aladdin> (accessed on 14 October 2020).
25. Jurafsky, D.; Martin, J. *Speech and Language Processing: An Introduction to Natural Language Processing, Computational Linguistics, and Speech Recognition*, 2nd ed.; Pearson Prentice Hall: Upper Saddle River, NJ, USA, 2009.
26. Ravi, V.; Madhav, V. Optimizing the reliability of a bank with Logistic Regression and Particle Swarm Optimization. *Data Manag. Anal. Innov.* **2021**, 91–107.
27. Breed, D.G.; Verster, T.; Schutte, W.D.; Siddiqi, N. Developing an Impairment Loss Given Default Model Using Weighted Logistic Regression Illustrated on a Secured Retail Bank Portfolio. *Risks* **2019**, *7*, 123. [CrossRef]
28. Abid, L.; Masmoudi, A.; Zouari-Ghorbel, S. The Consumer Loan's Payment Default Predictive Model: An Application of the Logistic Regression and the Discriminant Analysis in a Tunisian Commercial Bank. *J. Knowl. Econ.* **2018**, *9*, 948–962. [CrossRef]
29. Davis, L.; Harden, C. Factors Contributing to Bank Stability in Channelized, Alluvial Streams. *River Res. Appl.* **2014**, *30*, 71–80. [CrossRef]
30. Taha, Z. Bank Failure Prediction with Logistic Regression. *Int. J. Econ. Financ. Issues* **2013**, *3*, 537–543.
31. Chen, F.; Peng, H.; Chan, P.; Ma, X.; Zeng, X. Assessing the risk of windshear occurrence at HKIA using rare-event logistic regression. *Meteorol. Appl.* **2020**, *27*, e1962. [CrossRef]
32. Harris, C. A Comparative Analysis of Random Forest and Logistic Regression for Weed Risk Assessment. Master's Thesis, ProQuest Information Learning Co & University of Maryland, College Park, MD, USA, 2018.
33. Facile, I.; Galli, R.; Dinter, P.; Rosenberg, R.; Von Flüe, M.; Steinemann, D.C.; Posabella, A.; Droeser, R.A. Short- and long-term outcomes for primary anastomosis versus Hartmann's procedure in Hinchey III and IV diverticulitis: A multivariate logistic regression analysis of risk factors. *Langenbecks Arch. Surg.* **2021**, *406*, 121–129. [CrossRef] [PubMed]
34. Cuadrado-Godia, E.; Jamthikar, A.D.; Gupta, D.; Khanna, N.N.; Araki, T.; Maniruzzaman, M.; Saba, L.; Nicolaidis, A.; Sharma, A.; Omerzu, T.; et al. Ranking of stroke and cardiovascular risk factors for an optimal risk calculator design: Logistic regression approach. *Comput. Biol. Med.* **2019**, *108*, 182–195. [CrossRef] [PubMed]
35. Fügener, S.; Lang, A.; Gaber, T.; Burmester, G.; Buttgerit, F.; Hoff, P. THU0166 Logistic Regression Method Identifies RA as Risk Factors for Delayed Fracture-Healing—An Update of a Single-Center Retrospective Study. *Ann. Rheum. Dis.* **2015**, *74*, 254. [CrossRef]
36. Sing Tao Daily. Airstar: The Cumulative Number of Account Opening Applications Increased by Nearly 10 Times in the First Year of Opening. 2021. Available online: <https://www.singtao.ca/4994707/2021-06-10/news-%E8%99%9B%E9%8A%80airstar%E5%BC%9A%E9%96%8B%E6%A5%AD%E4%B8%80%E5%B9%B4%E7%B4%AF%E8%A8%88%E9%96%8B%E6%88%B6%E7%94%B3%E8%AB%8B%E9%87%8F%E5%A2%9E%E8%BF%9110%E5%80%8D/?variant=zh-hk> (accessed on 15 September 2021).
37. ZA Bank. About ZA Bank. 2021. Available online: <https://bank.za.group/en/hkno1virtualbank> (accessed on 21 September 2021).
38. Baidu Baike. WeBank. 2020. Available online: <https://baike.baidu.com/item/%E5%BE%AE%E4%BC%97%E9%93%B6%E8%A1%8C> (accessed on 30 October 2020).
39. WeBank. About Us. 2020. Available online: <https://www.webank.com/#/about> (accessed on 30 October 2020).
40. WeBank. About Us: Milestones. Available online: <https://www.webank.com/#/about/milestones> (accessed on 30 October 2020).
41. Sohu. Yao Huiya from WeBank: Fintech Breaks the Boundaries of Banking Business, Opening Banks Help Collaborative Innovation. 2020. Available online: https://www.sohu.com/a/397516866_115643 (accessed on 30 October 2020).
42. Sina Finance. WeBank Postpones Repayment for 3 Months to Help Small and Micro Businesses Overcome Difficulties. 2020. Available online: <http://finance.sina.com.cn/roll/2020-02-17/doc-iimxyqvz3488417.shtml> (accessed on 30 October 2020).
43. WeBank. About Us: Announcements, 2019 Annual Report. 2019. Available online: https://std.webankcdn.net/epss/upload/www/pdf/annual_report_2019_en.pdf (accessed on 30 October 2020).
44. InfoQ. The First Exposure of WeBank Internet Architecture. 2015. Available online: <https://www.infoq.cn/article/2015/10/WeBank-Interview> (accessed on 30 October 2020).

45. China Economic Net. Launched “We Yan Action”, WeBank Consolidated Compliance Operations. 2018. Available online: http://finance.ce.cn/bank12/scroll/201808/09/t20180809_29989338.shtml (accessed on 30 October 2020).
46. Monetary Authority of Singapore. What We Do. 2020. Available online: <https://www.mas.gov.sg/who-we-are/What-We-Do> (accessed on 31 October 2020).
47. Hong Kong Monetary Authority (HKMA). Virtual Banks. 2021. Available online: <https://www.hkma.gov.hk/eng/key-functions/banking/banking-regulatory-and-supervisory-regime/virtual-banks/> (accessed on 21 September 2021).
48. Monetary Authority of Singapore. 14 Digital Bank Applicants Eligible for Next Stage of Assessment. 2020. Available online: <https://www.mas.gov.sg/news/media-releases/2020/14-digital-bank-applicants-eligible-for-next-stage-of-assessment> (accessed on 27 November 2020).
49. Baidu Baike. Hong Kong (Special Administrative Region of the People’s Republic of China). 2020. Available online: <https://baike.baidu.com/item/%E9%A6%99%E6%B8%AF/128775?fr=aladdin> (accessed on 27 November 2020).
50. Baidu Baike. Singapore. 2020. Available online: <https://baike.baidu.com/item/%E6%96%B0%E5%8A%A0%E5%9D%A1/145065?fr=aladdin> (accessed on 27 November 2020).
51. Monetary Authority of Singapore. Guidelines on Risk Management Practices—Technology Risk. 2020. Available online: <https://www.mas.gov.sg/regulation/guidelines/technology-risk-management-guidelines> (accessed on 31 October 2020).
52. Monetary Authority of Singapore. Consultation Paper on Proposed Guidelines on Environmental Risk Management for Banks. 2020. Available online: <https://www.mas.gov.sg/publications/consultations/2020/consultation-paper-on-proposed-guidelines-on-environmental-risk-management-for-banks> (accessed on 31 October 2020).