Managing cybersecurity and technology risk is a major challenge for virtual banks. Although cyberattacks and a lack of system resilience can be detrimental for both traditional and virtual banks, they arguably have a greater impact on the latter. This is because virtual banks offer all their products and services online. The banking application is the only "storefront" for the entire banking service, and all transactions are completed at the customer’s fingertips.

Virtual banks must adopt a fit-for-purpose risk management approach that balances the simplicity and convenience of digital platforms and mobile applications with data protection, cybersecurity controls and a highly resilient IT infrastructure. By promoting trust through the use of the latest technology for IT delivery and cyberdefense, virtual banks can provide innovative, reliable and secure banking experiences to all their customers.

"With the benefits of a technology-driven operation and a cloud-native banking model, new customer experiences and financial inclusion can be achieved."

Virtual Banks vs. Traditional Banks

A virtual bank offers banking services primarily, if not entirely, through digital channels, including the Internet and mobile applications. Virtual banks have a limited physical presence; there are no brick-and-mortar branches, and all banking services are performed online. Depending on location, virtual banks are also known as neobanks or challenger banks. A virtual bank’s business operation is based on the application of financial technology (fintech) and innovation. Technology plays a pivotal role in determining what customers want and how their needs can be met. With the benefits of a technology-driven operation and a cloud-native banking model, new customer experiences and financial inclusion can be achieved. Virtual banks can be considered technology-driven financial services enterprises.

Today, nearly all conventional retail banks offer their customers some kind of digital experience. However, most of these service offerings are fragmented and replicate only a portion of the services available at a physical branch. Conventional retail banks have been successful operating in a traditional manner, mostly with legacy systems and infrastructure. Even among conventional retail banks with strong digital agendas, technology plays only a supporting role in enabling the technical functions required for business operations. At best, these enterprises are the front-runners of banks operating as technology firms (i.e., banks adopting fintech).

Virtual banks aspire to differ from conventional retail banks that offer online services in several ways:

- **Enhanced end-to-end customer experience**—Gone are the days of long lines at the local bank branch. With virtual banking, customers enjoy a seamless and efficient banking experience. The initial stage of virtual banking includes simple banking products and services, including fast account opening, competitive interest rates on deposits and

**DONALD TSE | CISA, CISM, CDPSE, CPA**

Has a passion for exploring the balance between innovation and cyberg and tech controls and making banking simpler and more intuitive. Tse focuses on virtual banking and is a founding member of Mox Bank, a virtual bank backed by Standard Chartered. He has extensive experience shaping and implementing business and technology risk strategies in investment banks such as Deutsche Bank, Credit Suisse and Nomura on a global and regional scale. As a certified public accountant (CPA) and a cyberprofessional, he offers a multidisciplinary approach to bridging the gaps between banking, cybersecurity and technology risk.
and attractive lending offers. Technology-driven virtual banks are working on leveraging big data analytics to approve loans more quickly, adopt fast payment systems, integrate with automated platforms to manage money and implement chatbots offering real-time banking experiences 24/7. The goal is to have an all-encompassing platform that is capable of handling the basic necessities in customers’ daily lives—shopping, food, accommodations, transportation, healthcare, insurance, bill payments, wealth management—all at the customers’ fingertips.

- **Technology-driven business model**—Innovative digital services do more than provide an interface between customers and the bank. The importance of regulatory technology (regtech) in supporting and facilitating the interface between banks and regulators cannot be understated. With the increasing complexity, scope and stringency of regulations around the globe and the growing volume of transactions and data that must be processed, this is the right time to automate compliance. For instance, the enhanced account-opening experience can only benefit by an electronic know-your-customer (eKYC) process, combined with big data analytics and machine learning to complement the fraud and antimoney laundering surveillance process. Virtual banking operations are technology-driven from front to back.

- **Agile ways of working**—The virtual bank’s operating model has shifted from a process-driven model to an agile way of working. In technology delivery, continuous deployment with small repetitive iterations allows the inclusion of improvements and lessons learned in each agile sprint. This model follows the spirit of innovation—start small, fail fast—and enables the rapid delivery of products and services. Cybersecurity practices also follow the agile way of working, including alignment of the security patching schedule and the review of security configurations. The agile way of working does not stop at technology delivery but encompasses all banking processes such as finance, operations and human resources (HR).

- **Promoting financial inclusion**—“Financial inclusion means that individuals and businesses have access to useful and affordable financial products and services that meet their needs—transactions, payments, savings, credit and insurance—delivered in a responsible and sustainable way.” Conventional retail banks achieve financial inclusion through their extensive branch networks, whereas virtual banks do so through their low marginal costs. Virtual banks have lower operating costs; for instance, unlike conventional retail banks, they do not have to pay rent for numerous branches, a cost savings that benefits their customers. Although the initial IT infrastructure for a virtual bank might be costly to set up, the scalability of robust IT systems reduces the incremental costs of attracting new customers. These cost savings can be passed on to customers by offering more attractive interest rates. The virtual bank, therefore, has no incentive to impose minimum account balance requirements or low-balance fees on its customers.

“Although the initial IT infrastructure for a virtual bank might be costly to set up, the scalability of robust IT systems reduces the incremental costs of attracting new customers.”

**Key Risk Factors Faced by Virtual Banks**

The emergence of virtual banking has changed the way banks operate, and the risk profile of a start-up virtual bank is different from that of an established conventional retail bank. With a heavy reliance on technology in the virtual bank business model, the key nonfinancial risk factors include:

- **Information and cybersecurity risk**—A new, fully digital bank is a high-profile target for cybercriminals. The many promotional events surrounding the launch of a new virtual bank can increase the likelihood of a cyberattack. For instance, a Chinese-based virtual bank suffered a distributed-denial-of-service (DDoS) attack on the first day of its launch, resulting in a significant delay in service.³ Data leakage and confidentiality breaches due to unauthorized access or cyberattack may result in legal costs and serious damage to the bank’s reputation. A successful cyberattack is a serious matter for a conventional...
Third-party risk—Adopting certain vendor products is unavoidable in a technology-driven business operation. Completing the cloud governance and third-party due diligence process can be a daunting task. It is critical to ensure vendors, regardless of their size, adhere to the bank’s level of cybercontrols. Thorough due diligence not only involves reviewing policies and standards, but it also includes onsite review of operations and control evidence. The bank’s legal counsel should also prepare standardized legal terms regarding the information security provisioning of the vendors. There is a certain complexity involved in maintaining continuous oversight of third parties on a large scale, particularly with Software as a Service (SaaS) vendors. However, it is important to remember that even though technology and activities are outsourced in a shared responsibility model, accountability is not outsourced. Accountability continues to rest with the bank’s board and senior management.

How to Mitigate Risk
A regulated virtual bank should have a low-risk appetite overall and a zero-risk appetite specifically for any major breaches. To reduce a bank’s risk profile, a holistic risk management approach should be in place, with several components:

• **Strong governance**—The tone at the top is crucial for risk management. Clear roles and responsibilities
and regular engagement with business leaders must be established. The existing risk management framework should be leveraged so that adjustments can be tailored to the virtual banking environment.

- **Clear guiding principles**—There are two categories of controls: mandatory and desirable. Mandatory controls should never be compromised, including customer confidentiality, protection of customers’ deposits and antimony laundering. Data encryption, secured configuration, timely patching and a highly resilient system architecture must be in place. This should also be aligned with the risk appetite level set by the board. Whether a control is mandatory or desirable also depends on the product delivery phase. A control requirement may be less stringent in a sandbox environment but mandatory in a real-world production environment. A regulatory sandbox is a framework set up by a regulator that allows fintech start-ups and other innovators to conduct live experiments in a controlled environment under a regulator’s supervision.6 For example, in terms of IT resilience, certain outages would be more acceptable in a sandbox environment.

- **Regular risk assessments and control testing**—Given the more dynamic business environment of a virtual bank, testing to detect control breaks must be conducted more regularly than in a conventional retail bank. When adopting a risk-based approach, material changes to the IT environment and key controls are subjected to a larger sampling size and more frequent and in-depth reviews, aligning with the agile way of working. Depending on the project stage, different types of risk assessments (e.g., rapid risk review, deep dive, read across) will be invoked. A cybersecurity and technology risk and control library should be established, making reference to internationally recognized frameworks such as COBIT® and the US National Institute of Standards and Technology (NIST) as the control baseline.

- **Remediation monitoring**—Close monitoring of remediation status should be in place to close any identified gaps. On the technology side, regular system snapshots, encrypted information transmission, and regular patching and review are crucial to ensure a stable and safe IT environment.

- **Risk awareness**—Risk management is everyone’s responsibility. Process owners should understand and follow the bank’s risk tolerances. A positive risk culture should be established, with career-related rewards for personnel to ensure individual accountability.

**Agile Risk Advisory Framework**

To strike a balance between enabling an innovative environment and operating safely, a phased approach that aligns with the agile way of working can be used (figure 1). The phased approach includes:

**FIGURE 1**

Agile Risk Advisory Framework
No new type of risk is introduced by virtual banking. But risk managers must be prepared to manage a different risk profile with a greater focus on technology. Risk can be managed once an appropriate risk appetite has been set, followed by regular risk identification and timely remediation. Making good use of regulatory sandboxes enables a new product or service to be tested in a controlled environment to ensure that any risk factors are discovered and managed.

Conclusion
Traditionally, banks are not very technology savvy. But a virtual bank is different from a conventional retail bank in many ways—from its method of operation to the customer experience it provides. More than a decade after the restructuring imposed by the 2008 financial crisis, the banking industry is now at the growth stage in terms of the adoption of technology. Due to the adoption of virtual banks, cybersecurity and technology risk professionals are facing a changing threat landscape that requires them to adapt their perspectives in evaluating and managing associated risk. The heightened cyber and technology resilience risk profiles require an advanced knowledge of tools, increased awareness and intelligent process integration.

Endnotes
3 “Ping An OneConnect Suffered a Cyber Attack on Its Opening Day,” Hong Kong Economic Journal, 5 October 2020, https://www1.hkej.com/features/article?q=%23%E8%99%9B%E6%93%AC%E9%8A%80%E8%A1%8C%E5%B8%B2%E5%A0%B4%E6%B6%88%E6%81%A9%23&suid=999880528
4 Qichang, C.; “WeLab Bank Suspends 9.8% Hong Kong Dollar Time Deposit Flash Event, Saying More Stress Tests Are Needed,” Hong Kong Economic Times, 10 September 2020, https://wealth.hket.com/article/2749151/WeLab%20Bank%E6%9A%AB%E5%81%9C9.8%E5%8E%98%E5%B8%AF%E5%B5%83%E5%AE%9A%E6%9C%9F%E5%AD%98%E6%AC%BE%E5%BF%AB%E9%96%83%E6%B4%BB%E5%BB%95%E3%80%80%E7%A8%B1%E9%9C%80%E9%80%B2%E8%A1%8C%E6%9B%B4%E5%A4%9A%E5%A3%93%E5%8A%9B%E6%B8%AC%E8%A9%A6%cc=aw
6 Consultative Group to Assist the Poor (CGAP), “Regulatory Sandboxes: What Have We Learned So Far?” 1 August 2019, https://www.cgap.org/blog/series/regulatory-sandboxes-what-have-we-learned-so-far