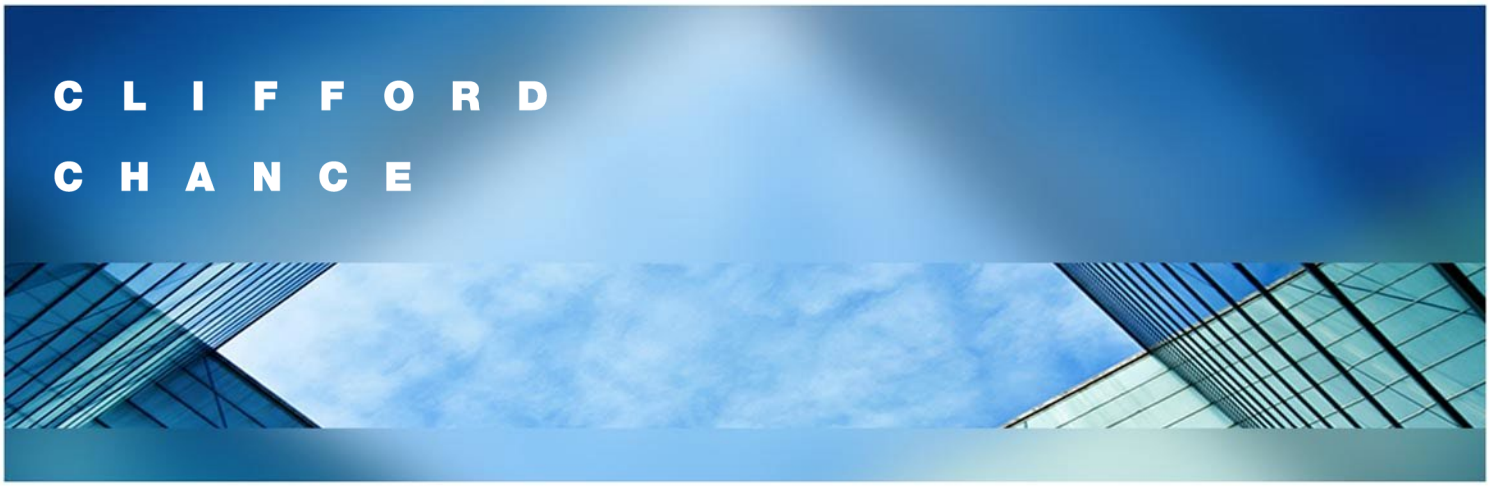

ENHANCING OPERATIONAL RESILIENCY OF FINANCIAL INSTITUTIONS IN SINGAPORE AND HONG KONG

Increasing cyber threats and the Covid-19 pandemic have underscored the importance of strengthening operational resiliency within the financial sector. In this briefing, we discuss recent major developments in Singapore and Hong Kong, which are relevant to financial institutions in their operational resiliency against disruptive events like cyber incidents, technology failures and pandemics.

Key issues

- Regulators in Singapore and Hong Kong have taken a proactive stance by issuing new guidance to enhance operational resiliency, taking into account learnings from navigating through the pandemic.
- In Singapore, regulatory guidance on technology risk management and business continuity management have been substantively revised. An information paper focusing on the management of risks arising from third party arrangements have also been published.
- Singapore also introduced additional measures to bolster the security of digital banking.
- In Hong Kong, a new supervisory policy manual on developing operational resilience framework for authorised institutions was published recently.
- Cybersecurity laws in Singapore and Hong Kong in relation to critical infrastructure are expected to be updated.

IMPORTANCE OF OPERATIONAL RESILIENCY

Financial institutions (FIs) today operate in an increasingly complex environment. The increased dependency on technology infrastructure, growing reliance on third party service providers and pandemic-related disruptions have exacerbated the operational risks faced by FIs, and underscore the need for FIs to effectively manage operational risks.

To enhance the operational resiliency of FIs in Singapore and Hong Kong, regulators in these jurisdictions have been continuously updating their guidance to FIs to account for the evolving operational risk landscape. We discuss below some of the measures which FIs operating in these jurisdictions ought to consider when thinking about enhancing their operational resiliency.

SINGAPORE

Technology Risk Management

Financial Services and Markets Act 2022

MAS currently relies on its powers spread across various Acts to impose requirements on technology risk management (TRM). The new Financial Services and Markets Act 2022 (FSM Act), which was passed in April 2022, consolidates and harmonises these powers by introducing a centralised power that empowers the MAS to impose requirements on TRM on any FI or classes of FIs in relation to the FI's system(s), irrespective of whether the system(s) supports a regulated activity.

For further details on the FSM Act, please see our client briefing on New Omnibus Act for Singapore's Financial Sector – Financial Services and Markets Act 2022.

Cybersecurity Act 2018

To enhance the cyber resiliency of critical informational infrastructure (CII) sectors in Singapore (which includes banking and finance), there will be a review of the Cybersecurity Act 2018 (CS Act). The review will look into expanding the scope of the CS Act to improve awareness of threats over Singapore's cyberspace, and protect virtual assets (e.g. systems hosted on the cloud) as CII if they support essential services. Besides CII, the review will also cover foundational digital infrastructure and key digital services. A public consultation is expected to take place in early 2023.

Business Continuity Management

Guidelines on Business Continuity Management (BCM Guidelines)

Earlier last year, the MAS revised its TRM Guidelines to guide FIs in implementing a more robust technology risk management (TRM) framework. More recently, the MAS revised its BCM Guidelines to help FIs strengthen their resilience against service disruptions.

Among other things, the revised BCM Guidelines:

- introduces a new concept of "business service" which is tied to the service which the FI provides to its external customers. FIs are required to identify its critical business services and determine recovery strategies and resource allocation based on criticality;
- require FIs to establish a Service Recovery Time Objective (SRTO) for each critical business service, taking into consideration its obligations to customers;
- identify and map end-to-end dependencies that support each critical business service. These dependencies should cover people, processes, technology and other resources, including those involving third parties;
- review the critical business services and their STROs and dependencies at least annually, or whenever there are material changes that affect them;
- audit its overall BCM framework and the BCM of each critical business services at least once every three years. The audit should be conducted by an independent qualified party, and the audit reports submitted to MAS upon request; and
- require senior management to provide an annual attestation to the Board on the state of the FI's BCM preparedness. The attestation should be provided to the MAS upon request.

Given the increasingly complex and interconnected operating environment of FIs, the conventional approach of identifying and planning based on critical business functions may not be sufficient anymore, as interdependencies across functions could be missed, impeding the recovery of a critical business service during a disruption. As such, MAS has revised the BCM Guidelines to shift the focus of BCM to a service-centric approach.

The revised BCM Guidelines were issued on 6 June 2022 and supersedes its previous version. FIs are expected to meet the BCM Guidelines within 12 months from its issuance. FIs should also establish their BCM audit plan within 12 months, and the first BCM audit should be conducted within 24 months of the issuance of the BCM Guidelines.

Measures to Bolster the Security of Digital Banking

In view of the growing threat of online scams targeting bank customers, MAS and the Association of Banks in Singapore (ABS) introduced two rounds of additional measures to bolster the security of digital banking in the span of six months.

From January 2022, banks are required to take urgent steps to put in place more stringent measures to prevent and detect scams, as well as effective incident handling and customer service. These measures include the removal of clickable links in emails or SMSes sent to retail customers.

In June 2022, the MAS and ABS announced additional measures to safeguard customers from digital banking scams. These additional measures are to be progressively implemented by 31 October 2022, and include providing an emergency self-service "kill-switch" for customers to suspend their bank accounts quickly, and facilitating rapid account freezing and fund recovery operations.

While the above measures apply to retail banks in Singapore only, MAS expects all FIs to have in place robust measures to prevent and detect scams, as well as effective incident handling and customer service in the event of a scam. FIs should therefore consider if the abovementioned measures are relevant to their business and implement them accordingly.

Third Party Risk Management

Information Paper on Operational Risk Management – Management of Third Party Arrangements

In August 2022, the MAS published an information paper setting out MAS' supervisory expectations, good practices, improvement areas and case examples on operational risk management with a focus on third party risk management, following a thematic inspection of selected banks over 2020 and 2021.

All banks are expected to benchmark their practices against the information paper, and take steps to address any gaps in a risk-appropriate manner, while non-bank FIs are encouraged to adopt the recommended practices where relevant and appropriate to the materiality of the risks posed by their third party arrangements.

HONG KONG

Guidance on Operational Resilience

FIs in Hong Kong have exhibited a high level of operational resiliency owing to business continuity plan (BCP) preparations and adoption of financial innovations during the first two years of the pandemic[1]. Recognising the importance for FIs to ensure continued strength and achieve operational resilience objectives, the Securities and Futures Commission (SFC) published circulars in both February and March 2022 to remind licensed corporations of the importance of BCP amidst the latest pandemic situation. Amongst others,

[1] Hong Kong Institute for Monetary and Financial Research (HKIMR) report on "COVID-19 and the Operational Resilience of Hong Kong's Financial Services Industry: Preliminary considerations from the 2020-2021 experience" (HKIMR Report), June 2022

the SFC also reminded intermediaries of the expected standards published in its October 2021 circular, namely:

- intermediaries should have an effective governance framework in place to set their operational resilience objectives, as well as measures to identify disruptive incidents on an ongoing basis and respond and adapt to disruptive incidents;
- intermediaries should have an effective operational risk management framework in place to assess the potential impact of disruptions on operations and compliance matters and manage the resulting risks;
- intermediaries' information and communication technology systems are expected to be resilient in order to support the effective operations of their business in the event of disruptions; such systems should operate in a secure and adequately controlled environment. This covers both software and hardware considerations;
- intermediaries are expected to identify their dependencies on key third parties (including intragroup entities), evaluate the resilience of third-party service providers and manage the resulting risks in accordance with their operational resilience objectives; and
- intermediaries are expected to have an effective BCP in place and review the plan at least annually to assess whether revisions are necessary in light of any relevant material changes. Intermediaries should also adopt an effective incident management process on disruptive incidents so as to prevent their recurrence or mitigate their severity.

To set out the Hong Kong Monetary Authority (HKMA)'s supervisory approach to operational resilience and provide authorized institutions (AIs) with guidance on the general principles which AIs are expected to consider when developing their operational resilience framework, the HKMA issued a new supervisory policy manual (SPM) on operational resilience on 31 May 2022 (OR-2 module). The module serves to implement the Basel Committee on Banking Supervision's Principles for Operational Resilience from March 2021. To complement the OR-2 module, the HKMA also revised its SPMs on business continuity planning and operational risk management. To this end, every AI is expected to:

- have developed its operational resilience framework and determined the timeline by which it will become operationally resilient by 31 May 2023; and
- become operationally resilient as soon as its circumstances allow and not later than three years after the initial one-year planning period, i.e. no later than 31 May 2026.

Technology Risk Management

As part of the HKIMR Report, an industry survey conducted in July 2021 showed that whilst respondents recognised technology as being essential for new staff deployment strategies and further digitalisation of their services, they were aware of the potential risks related to cybersecurity, data security and data privacy.

Currently, Hong Kong does not have specific legal requirements on the cyber security of critical infrastructure. On 20 July 2022, the cybercrime sub-committee of the law reform commission began a three-month consultation on

cyber-dependent crimes, having considered the law of seven other jurisdictions namely Australia, Canada, England and Wales, Mainland China, New Zealand, Singapore and the United States. The preliminary proposals for law reform aim to address the challenges to protecting individuals' rights caused by the rapid developments associated with information technology, computers and the internet.

CONCLUSION

The Covid-19 pandemic has escalated the need for more robust management of operational risks within the financial sector. In Singapore and Hong Kong, regulators have taken a proactive stance by issuing new guidance to enhance operational resiliency, taking into account learnings from navigating through the pandemic. Such guidance also contains updated measures to address heightened cybersecurity threats, amid increasing digitalisation and growing cases of cyber incidences. FIs operating in these jurisdictions can benefit by reviewing their operations against these updated guidance and implementing the necessary changes to mitigate their operational risks.

CONTACTS

Lena Ng
Partner

T +65 6410 2215
E lena.ng
@cliffordchance.com

Janice Goh
Partner,
Cavenagh Law LLP*

T +65 6661 2021
E janice.goh
@cliffordchance.com

Matthias Feldmann
Partner

T +852 2825 8859
E matthias.feldmann
@cliffordchance.com

Viola Lui
Partner

T +852 2825 8842
E viola.lui
@cliffordchance.com

Rocky Mui
Partner

T +852 2826 3481
E rocky.mui
@cliffordchance.com

Mark Shipman
Partner

T +852 2825 8992
E mark.shipman
@cliffordchance.com

Donna Wacker
Partner

T +852 2826 3478
E donna.wacker
@cliffordchance.com

Michael Wang
Partner

T +852 2826 3564
E michael.wang
@cliffordchance.com

Jonathan Wong
Partner

T +852 2825 8841
E jonathan.wong
@cliffordchance.com

Teoh Mae Yen
Counsel

T +65 6410 2224
E maeyen.teoh
@cliffordchance.com

Samuel Kwek
Associate

T +65 6506 1963
E samuel.kwek
@cliffordchance.com

Yaru Chia
Associate

T +65 6410 2223
E yaru.chia
@cliffordchance.com

Michelle Lee
Associate

T +65 6506 2790
E michelle.lee
@cliffordchance.com

Allison Tan
Associate

T +65 6661 2090
E allison.tan
@cliffordchance.com

Sheena Teng
Professional Support
Lawyer

T +65 6506 2775
E sheena.teng
@cliffordchance.com

www.cliffordchance.com

Clifford Chance Pte Ltd
12 Marina Boulevard, 25th Floor Tower 3
Marina Bay Financial Centre
Singapore 018982