OPTIMA
Supporting Success

SFC Circular Summary
Operational Resilience and Remote Working

On 4 October 2021, the SFC released a circular on operational resilience and remote working, referring to LC's ability to prevent, adapt, recover and learn from operational disruptions, particularly in light of the COVID-19 pandemic.

The circular, together with its appendices, set out SFC's operational resilience standards, including required implementation measures, as well as regulatory standards expected for managing and mitigating major possible risks of remote working.

The circular also encourages LCs to read its accompanying Report on Operational Resilience and Remote Working Arrangements which sets out case examples and lessons learned drawn from SFC's review of some LCs' operational resilience measures during the COVID-19 pandemic and other disruptive events. It also explains the major possible risks of remote working and provides suggested techniques and procedures for risk mitigation. Intermediaries are encouraged to adopt the suggested techniques and procedures where appropriate in their circumstances.

Circular Summary

Operational Resilience Standards

The SFC provided its operational resilience standards and required implementation measures which supplement its existing guidance as set out below.

Operational Resilience Standards	Required Implementation Measures
Governance - Implementation of an effective governance framework to: ▪ set operational resilience objectives; ▪ develop, implement and oversee arrangements and measures to identify on an ongoing basis disruptive incidents which may affect the sound, efficient and effective operations of business; and ▪ respond and adapt to disruptive incidents	LCs to ensure: - Senior management assume full responsibility for setting operational resilience objectives and developing and implementing the necessary arrangements and measures - Staff members designated to monitor the ongoing operational resilience business units in support of the senior management's oversight - Senior management are provided with sufficient information to continually and in a timely manner assess matters which may affect the LC's operational resilience and consider and approve any necessary adjustments to its operational resilience efforts
Operational Risk Management - Implementation of an effective operational risk management framework to: ▪ assess the potential impact of disruptions on operations (including people, processes and	LCs should: - Establish and maintain effective policies and procedures to ensure proper management of operational risks to which they are exposed

systems) and compliance matters; and ▪ manage the resulting risks in accordance with operational resilience objectives	- conduct periodic comprehensive to ensure that the risk of losses resulting from operational disruptions is maintained at acceptable and appropriate levels
Information & Communication Technology (ICT) Including Cybersecurity - Ensuring that the ICT systems: ▪ are resilient in order to support the sound, efficient and effective business operations in the event of disruptions; and ▪ operate in a secure and adequately controlled environment	LCs to ensure: - Establishment of policies and procedures for ensuring the secure operation of their ICT systems to protect the confidential data and information in their possession - Management of cybersecurity risks on an ongoing basis
Third-Party Dependency Risk Management - Identifying dependencies on key third parties, including intragroup entities, for the sound, efficient and effective business operations - Evaluating the resilience of third-party service providers and managing the resulting risks in accordance with operational resilience objectives	LCs should: - Taking appropriate steps to identify, contain and manage third-party dependency risks - Conduct reviews at suitable intervals and whenever there are changes in key service providers, to ensure that any risk of suffering losses (whether financial or otherwise) as a result of third-party dependencies is maintained at acceptable and appropriate levels
Business Continuity Plan (BCP) and Incident Management - Implementation of an effective BCP in place to respond to, adapt to and recover from disruptive incidents - Reviewing the BCP at least annually to assess whether revisions are necessary in light of any material changes to the LC's operations, structure or business - Adopting an effective incident management process to identify, assess, rectify and learn from disruptive incidents as well as to prevent their recurrence or mitigate their severity	LCs should: - Establish and maintain a BCP which should address the various disruptive scenarios identified and set out corresponding procedures for activating the plans - Review the BCP at least annually and whenever necessary and properly documenting the review results - Revise the BCP in light of changes to the LC's operations, structure or business - Develop an incident management process, which would be triggered upon the occurrence of a disruptive incident, to address: ▪ the applicable reporting and escalation procedures; ▪ the determination of appropriate actions for responding to the incident; ▪ the identification of the root cause through an analysis of the incident; ▪ the prevention of the occurrence of a similar incident and the need to mitigate its severity if it does occur; and

	▪ the implementation of communication plans to report incidents to internal and external stakeholders, including reporting to the regulator material incidents which affect their clients' interests and their ability to continue conducting business as usual.

Managing and Mitigating Remote Working Risks – Expected Regulatory Standards

The SFC notes that there are various control and oversight risks unique to working from home (WFH). Set out below are SFC's expected regulatory standards for managing and mitigating these risks as well as suggested implementation techniques and procedures. However, it should be noted that LCs should put in place proper governance and oversight mechanisms commensurate with their size and internal organisation to ensure the effectiveness of the techniques and procedures adopted.

Major Possible Risks	Expected Regulatory Standards
Governance Resources and Capacity: - Insufficient or inappropriately planned resources - Inferior networking equipment may increase risk of failing time sensitive trading activities Supervision or control processes: - Delay in identification of compliance issues due to suspension or deferral of compliance reviews - Lack of in-person supervision and controls by trading desk supervisors may lead to heightened market misconduct risk	LCs should ensure: - Sufficient resources for the proper performance of work from remote locations are in place before shifting staff to remote working - Ensuring that there is an appropriate minimum staff presence in the office for business and operational systems, which are considered high risk or otherwise not fit to be performed from remote locations - Policies, procedures and controls are reviewed and updated on a regular basis and whenever necessary - IT infrastructure, systems, software, hardware, network capacity and connectivity provided to support efficient remote working are appropriate and adequate
Off-Premises Trading - Non-compliant behaviour due to lowered system support in respect of transaction reporting, trade surveillance and suspicious transaction monitoring - Increased risk of trading malpractice and market misconduct due to undetected intentional or reckless use of unmonitored or unencrypted communication applications for sharing confidential trading	LCs should: - Establish and maintain effective policies and procedures, oversight mechanism, systems and controls to ensure the integrity and compliance with all regulatory requirements before allowing staff to conduct any off-premises trading activities - Carry out proactive compliance oversight for off-premises trading activities by independent compliance or audit functions - Stringently review remote-working staff's adherence to the compliance policies,

information by staff who conduct off-premises trading activities	procedures and controls in relation to off-premises trading
Outsourcing and Third-Party Arrangements - Third party failure to provide adequate remote working arrangement support as required by an LC	LCs should: - Establish and maintain effective policies and procedures to ensure the proper selection and appointment of key third parties to support remote working arrangements and the proper management and monitoring of all the risks they pose in a remote working environment
Information Security - Increased risk of leakage of client information and other confidential information in WFH environment due to numerous factors (e.g. taking/ disposing of hard copies out of office; remote printing; use of removable drives for data storage)	LCs should: - Implement appropriate and effective data security policies, procedures and controls to prevent and detect the occurrence of unauthorised insertion, alteration or deletion of data processing systems and data in a remote working environment - Ensure that operating and information management systems are secure and adequately controlled for remote working - Ensure that remote access to client information and other confidential information on a need-to-know basis is strictly enforced
Cybersecurity - Increased risk of IT system attacks (e.g. malware and ransomware attacks) due to use of out of office internet connections and personal devices in WFH environment	LCs should: - Establish appropriate measures to manage and mitigate the cybersecurity risks associated with remote working arrangements, as well as prevent and detect cybersecurity threats
Record Keeping - Increased risk of delay, impairment and fragmentation of certain types of records required to be kept pursuant to regulatory requirements - Possible breach of s130 SFO record keeping premises requirements due to records and documents held by remote-working staff not being sent back to the LC's approved office premises	LCs should: - Implement and maintain appropriate internal controls to ensure that where a staff can remotely access its trading or other systems, the activities conducted by the staff on these systems are effectively captured in the records and documents generated by these systems. - Put in place effective policies, procedures and controls for the records and documents to be sent back by the staff to approved premises for the purpose of section 130 of the SFO as soon as practicable
Notification Obligations - LCs are required to notify SFC of significant changes in their business plans covering internal controls, organisational structures, contingency plans and related matters,	LCs should: - Implement measures to promptly notify the SFC of the implementation of remote working arrangements which constitute significant changes in their business plans

including shifting staff to remote working where it constitutes a material change in their business plans. LCs may overlook this notification requirement when a remote working arrangement is deployed for a short period of time	and any significant changes in these arrangements
WFH Arrangements - Increased risk of potential unlawful disclosure of client information, proprietary information or other confidential information by WFH staff to family members, neighbours and friends visiting the home office - Higher risk of network instability because residential networking equipment and software (e.g., WIFI routers) may not have the same depth or breadth of features as the equipment and software installed in the LC's office for commercial use - Residential networks may be exposed to a wider range of threats (such as malware).	LCs should: - Establish and maintain adequate internal controls and operational capabilities which are necessary to mitigate any additional risks unique to WFH arrangements - Establish and maintain policies, procedures and controls which are strictly enforced for WFH staff to access client information and other confidential information on a need-to-know basis - Provide specific training to WFH staff on the policies and procedures for protecting the secrecy of confidential information in a home office environment

In its circular, the SFC has encouraged LCs to adopt the suggested techniques and procedures, outlined above, where appropriate in their circumstances.