SECURITIES AND FUTURES COMMISSION
證券及期貨事務監察委員會

Circular

4 October 2021

Circular to intermediaries

Operational resilience and remote working

Intermediaries' operational resilience, which refers to their ability to prevent, adapt and respond to and recover and learn from operational disruptions, has been stress-tested by the COVID-19 pandemic. While the guidance provided by the Securities and Futures Commission (SFC) on cybersecurity, business continuity plans, internal controls and risk management in its codes, guidelines and circulars[1] has helped licensed corporations maintain resilience amid the COVID-19 outbreak, it is important for them to ensure continued strength by adopting a comprehensive approach to achieve their operational resilience objectives based on common established standards.

For example, many intermediaries transitioned to hybrid working arrangements during the pandemic, with employees working partly from the office and partly from home or other remote locations (ie, remote working). Many intermediaries are considering whether to maintain some form of hybrid working arrangement as a new normal after the pandemic. Intermediaries should be vigilant about the risks involved and implement appropriate risk management measures and internal controls to address them.

Appendix A to this circular provides operational resilience standards and required implementation measures which supplement the SFC's existing guidance. Appendix B sets out the expected regulatory standards for managing and mitigating some major possible risks of remote working.

Intermediaries are also encouraged to read the Report on Operational Resilience and Remote Working Arrangements which accompanies this circular. The report aims to provide intermediaries with a better understanding of the regulatory standards and required implementation measures for operational resilience. In addition to providing suggested techniques and procedures, the report shares case examples and lessons learned drawn from the SFC's review of some licensed corporations' 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.

Should you have any questions regarding this circular, please contact your case officers-in-charge or Ms Seine Luk at 2231 1696.

[1] For example, the Code of Conduct for Persons Licensed by or Registered with the Securities and Futures Commission, Fund Manager Code of Conduct, Management, Supervision and Internal Control Guidelines for Persons Licensed by or Registered with the Securities and Futures Commission, Circular to All Licensed Corporations on Alerts for Ransomware Threats issued on 15 May 2017, Circular to Intermediaries on Receiving Client Orders through Instant Messaging issued on 4 May 2018 and Circular to Licensed Corporations on Management of Cybersecurity Risks Associated with Remote Office Arrangement issued on 29 April 2020.

Intermediaries Supervision Department
Intermediaries Division
Securities and Futures Commission

Enclosure

End

SFO/IS/024/2021

Appendix A

Operational resilience standards and required implementation measures

1. Operational resilience standard 1: Governance

Intermediaries should have an effective governance framework in place to set their 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 their business, and respond and adapt to disruptive incidents.

Required implementation measures

1.1 Intermediaries' senior management assume full responsibility for setting operational resilience objectives and developing and implementing the necessary arrangements and measures.

1.2 Designated staff members should monitor the ongoing operational resilience of the intermediary's business units in support of the senior management's oversight.

1.3 The senior management should be provided with sufficient information to enable them to continually and in a timely manner assess matters which may affect the intermediary's operational resilience and consider and approve any necessary adjustments to its operational resilience efforts.

2. Operational resilience standard 2: Operational risk management

Intermediaries should have an effective operational risk management framework in place to assess the potential impact of disruptions on operations (including people, processes and systems) and compliance matters and manage the resulting risks in accordance with their operational resilience objectives.

Required implementation measures

2.1 Intermediaries should establish and maintain effective policies and procedures to ensure the proper management of operational risks to which they are exposed. They should also conduct comprehensive reviews at suitable intervals to ensure that the risk of losses resulting from operational disruptions is maintained at acceptable and appropriate levels.

3. Operational resilience standard 3: Information and communication technology (ICT) including cybersecurity

Intermediaries should ensure that their ICT systems are resilient in order to support the sound, efficient and effective operations of their business in the event of disruptions, and that these systems operate in a secure and adequately controlled environment.

Required implementation measures

3.1 Intermediaries should establish policies and procedures for ensuring the secure operation of their ICT systems to protect the confidential data and information in their possession, and manage cybersecurity risks on an ongoing basis.

4. Operational resilience standard 4: Third-party dependency risk management

Intermediaries should identify their dependencies on key third parties, including intragroup entities, for the sound, efficient and effective operations of their business, evaluate the resilience of third-party service providers and manage the resulting risks in accordance with its operational resilience objectives.

Required implementation measures

4.1 Intermediaries should take appropriate steps to identify, contain and manage third-party dependency risks. Reviews should be conducted at suitable intervals and whenever there are changes in key service providers, to ensure that the intermediary's risk of suffering losses, whether financial or otherwise, as a result of third-party dependencies is maintained at acceptable and appropriate levels.

5. Operational resilience standard 5: Business continuity plan and incident management

Intermediaries should have an effective business continuity plan in place to respond to, adapt to and recover from disruptive incidents and review the plan at least annually to assess whether revisions are necessary in light of any material changes to the intermediary's operations, structure or business. They should also adopt 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.

Required implementation measures

5.1 Intermediaries should establish and maintain business continuity plans which should:

(a) address the various disruptive scenarios identified and set out corresponding procedures for activating the plans; and

(b) be reviewed at least annually and whenever necessary, and revised in light of changes to the intermediary's operations, structure or business. The review results should be properly documented.

5.2 Intermediaries should develop an incident management process, which would be triggered upon the occurrence of a disruptive incident, to address:

(a) the applicable reporting and escalation procedures;

(b) the determination of appropriate actions for responding to the incident;

(c) the identification of the root cause through an analysis of the incident;

(d) the prevention of the occurrence of a similar incident and the need to mitigate its severity if it does occur; and

(e) 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.

Appendix B

Expected regulatory standards for managing and mitigating remote working risks

1. Governance

Resources and capacity

1.1 Intermediaries should ensure that sufficient resources for the proper performance of work from remote locations are in place before shifting staff to remote working.

1.2 Intermediaries should establish and maintain effective policies and operational procedures and controls to cater for the needs of staff in different business units and operational functions who are working from remote locations. They should also ensure an appropriate minimum staff presence in the office for business or operational functions which are considered high risk or otherwise not fit to be performed from remote locations. These policies, procedures and controls should be reviewed and updated on a regular basis and whenever necessary.

1.3 Intermediaries should ensure that the IT infrastructure, systems, software, hardware, network capacity and connectivity provided to support efficient remote working are appropriate and adequate.

Supervision or control processes

1.4 Intermediaries should establish and maintain effective supervision and control processes to ensure staff's compliance with applicable legal and regulatory requirements as well as their own internal policies and procedures in remote working environments, including providing proper training to staff for performing their supervision or control functions remotely. They should also have the necessary skills and resources including access to all necessary records and documentation to effectively carry out their duties in remote working environments.

1.5 Prior to transitioning to remote working arrangements, intermediaries should put in place adequate compensating controls for any controls which will be suspended for remote-working staff.

1.6 Intermediaries should ensure that staff performing the compliance function in remote working environments establish, maintain and enforce effective compliance procedures, including appropriate surveillance systems for transactions, electronic communications and telephone calls, to detect breaches of the legal and regulatory requirements or the intermediary's own policies and procedures. Business or operational functions which are most susceptible to abuse and fraud should be closely monitored.

2. Off-premises trading

2.1 Before allowing staff to conduct any off-premises trading activities[1], intermediaries should establish and maintain effective policies and procedures, oversight mechanism systems and controls to ensure the integrity of these activities and their compliance with all regulatory requirements.

2.2 Where staff are allowed to conduct off-premises trading activities for agency orders or internally generated orders (eg, for proprietary accounts and staff accounts), the policies and procedures should ensure that remote-working staff use a recorded phone line to receive agency orders. Where the intermediary has not implemented a call recording system at remote locations, remote-working staff should immediately call back to the intermediary's telephone recording system in the office to record the time of receipt and order details. Where an intermediary has adopted remote working arrangements as a new norm for its trading staff, it should equip staff who receive telephone orders from clients with appropriate information and communication technology equipment including telephone recording.

2.3 Where staff are allowed to conduct off-premises trading activities for client orders, the policies and procedures should also ensure that:

- there are appropriate measures for complying with the requirements set out in the Circular to Intermediaries - Receiving Client Orders through Instant Messaging issued on 4 May 2018; and

- staff can access the trading and all other systems which are necessary for them to manage the overall order execution process and determine the execution strategy and parameters to execute client orders promptly and on the best available terms.

2.4 Where staff are allowed to conduct off-premises trading activities for proprietary accounts for back-to-back transactions with a client concerning an investment product, the policies, procedures and controls should ensure that staff can access all the necessary systems which enable them to obtain in a timely manner the information needed to determine the amount of trading profit to be disclosed to clients prior to or at the point of entering into these back-to-back transactions.

2.5 Independent compliance or audit functions, in close coordination with senior management, business operations, risk management and other relevant control functions, should carry out proactive compliance oversight for off-premises trading activities. Remote-working staff's adherence to the compliance policies, procedures and controls in relation to off-premises trading should be subject to stringent review processes.

[1] Registered institutions should discuss with the Hong Kong Monetary Authority (HKMA) before implementing off-premises trading as general practice.

3. Outsourcing and third-party arrangements

3.1 Intermediaries 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.

4. Information security

4.1 Before allowing staff to work remotely, intermediaries should implement appropriate and effective data security policies, procedures and controls to prevent and detect the occurrence of errors or omissions or the unauthorised insertion, alteration or deletion of, or intrusion into, their data processing systems and data (covering all confidential information in the intermediary's possession such as clients' personal and financial information and price sensitive information) in a remote working environment. Intermediaries should also ensure that their operating and information management systems are secure and adequately controlled for remote working.

4.2 Intermediaries should ensure that remote access to client information and other confidential information on a need-to-know basis is strictly enforced.

5. Cybersecurity

5.1 Intermediaries should establish appropriate measures to manage and mitigate the cybersecurity risks associated with remote working arrangements, as well as prevent and detect cybersecurity threats, having regard to the Circular on Management of Cybersecurity Risks Associated with Remote Office Arrangements issued on 29 April 2020.

6. Record keeping

6.1 Licensed corporations 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.

6.2 Before allowing remote-working staff to temporarily keep certain requisite records and documents at home or in other remote-working locations which are not approved premises for the purpose of section 130 of the Securities and Futures Ordinance, licensed corporations should put in place effective policies, procedures and controls for these records and documents to be sent back by the staff to approved premises as soon as practicable.

7. Notification obligation

7.1 Intermediaries should implement measures to promptly notify the Securities and Futures Commission and where applicable the HKMA of the implementation of remote working arrangements which constitute significant changes in their business plans and any significant changes in these arrangements.

8. Working-from-home (WFH) arrangements

8.1 Intermediaries should establish and maintain adequate internal controls and operational capabilities which are necessary to mitigate any additional risks unique to WFH arrangements.

8.2 Intermediaries should also 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.

8.3 Intermediaries should provide specific training to WFH staff on the policies and procedures for protecting the secrecy of confidential information in a home office environment.