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

Report on Operational Resilience and Remote Working Arrangements

October 2021

Contents

Introduction

1. During the COVID-19 pandemic, the Securities and Futures Commission (SFC) held extensive supervisory discussions with licensed corporations on:

   - Split-team arrangements to maintain business as usual of critical operations and services in the event office and business locations were inaccessible or of other pandemic-related disruptions;
   - Working-from-home (WFH) arrangements and compliance with conduct requirements; and
   - Operational resilience to cope with market dislocations and pandemic-related disruptions.

2. We noted that licensed corporations exhibited a strong level of resilience which helped them maintain business as usual during the pandemic. Remote working, particularly WFH, was found to be part of many licensed corporations' business continuity strategies.

3. We also observed that the SFC's guidance on cybersecurity, business continuity plans, internal controls and risk management in its codes, guidelines and circulars[1] has helped licensed corporations maintain resilience.

4. To ensure continued strength, it is important for intermediaries to adopt a comprehensive approach to achieve their operational resilience objectives based on common established standards. These include their ability to prevent, adapt and respond to and recover and learn from operational disruptions.

5. In addition, as remote working, particularly WFH, is likely to remain popular even after the pandemic is under control, intermediaries should be vigilant about the risks associated with remote working and implement appropriate risk management measures and internal controls to address these risks.

6. To these ends, in addition to discussing our supervisory observations, this report:

   (a) lays down operational resilience standards and required implementation measures which supplement the SFC's existing guidance. Suggested techniques and procedures as well as case examples and lessons learned drawn from our review of some licensed corporations' operational resilience plans and measures

[1] For example, the Code of Conduct for Persons Licensed by or Registered with the Securities and Futures Commission (Code of Conduct), Fund Manager Code of Conduct, Management, Supervision and Internal Control Guidelines for Persons Licensed by or Registered with the Securities and Futures Commission (Internal Control Guidelines), 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.

during the COVID-19 pandemic and other disruptive events are also provided; and

(b) sets out the expected regulatory standards for managing some major possible risks of remote working and provides suggested techniques and procedures to assist intermediaries' compliance with these standards.

7. While there may be alternative ways to achieve operational resilience objectives and mitigate the risks of remote working, intermediaries are encouraged to adopt the suggested techniques and procedures as appropriate to their circumstances.

Registered institutions should comply with all applicable requirements and should also make reference to other guidance issued by the Hong Kong Monetary Authority (HKMA) from time to time.

Operational resilience

1. Intermediaries are exposed to a wide range of disruptive events which may affect their operations. These events range from the breakdown of a single computer, which affects an individual staff member's ability to provide services, to cybersecurity incidents or pandemics, which can lead to a wide-scale disruption of an intermediary's activities.

2. Some disruptions are unavoidable. Therefore, intermediaries should have a proper framework in place to identify, prepare for, respond and adapt to disruptive incidents.

3. This section sets out a set of operational resilience standards and required implementation measures for attaining these standards.

4. To assist intermediaries in complying with the operational resilience standards and required implementation measures, we have also provided some suggested techniques and procedures as well as case examples and lessons learned drawn from our supervisory observations.

5. Intermediaries may wish to consider whether the suggested techniques and procedures and practices are applicable to their own circumstances. In any event, intermediaries should implement all necessary policies, procedures and controls which are commensurate with their business size and complexity, and effective for complying with the operational resilience standards and required implementation measures.

Operational resilience standard 1: Governance

Operational resilience standard 1
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[2], and respond and adapt to disruptive incidents.

Required implementation measures
Intermediaries' senior management assume full responsibility for setting operational resilience objectives and developing and implementing the necessary arrangements and measures[3]. Designated staff members should monitor the ongoing operational resilience of the intermediary's business units in support of the senior management's oversight.

2 Part I of the Internal Control Guidelines.

3 Paragraph I(1) of the Internal Control Guidelines.

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[4] and consider and approve any necessary adjustments to its operational resilience efforts.

Suggested techniques and procedures

6. Senior management oversight arrangements are put in place to:

   (a) identify disruptive scenarios related to internal processes, people, systems, external threats and third parties which may affect the intermediary's ability to continue to conduct business activities or provide services;

   (b) review and approve the intermediary's risk tolerance for disruptions to its business operations by senior management, having regard to its risk profile and the capabilities of various operational environments, including systems, processes, people, IT infrastructure and risk management, to support operational resilience; and

   (c) develop and implement effective and resilient systems and controls for maintaining business activities and services which are consistent with the intermediary's tolerance for disruption.

Case examples

7. Some firms assigned senior management, responsible officers or department heads to be responsible for identifying and reviewing critical functions and systems and updating written business contingency plans annually or whenever there is a change to services, systems or staff. They also ensured that their business contingency plans properly covered potential disruptive events and the corresponding response measures, giving higher priority to critical functions and systems such as those related to trading and settlement.

8. The senior management of a firm regularly reviewed the implementation measures for adapting to disruptive incidents to ensure that these measures could enable the firm to carry out its business in an efficient and effective manner. For example, at the onset of the COVID-19 pandemic, the firm adopted split-site operations to physically segregate staff among the firm's office premises, recovery site and home offices. Staff were required to work at their designated work locations for multiple weeks before rotation to minimise the potential impact of a confirmed COVID-19 infection in any of these work locations. Upon review, the firm found that the split-site operations created obstacles to effective communication among staff and promptly shortened the rotation cycle. This gave managers greater flexibility in managing workload, promoted better communication and accommodated staff's personal needs.

[4] Paragraph I(2) of the Internal Control Guidelines.

9. During the pandemic, a firm experienced resource constraints and some audit reviews could not be conducted as scheduled. In response, the firm set up an assessment committee to identify key risk areas in its operations and prioritise reviews of these areas which included operational resilience and WFH (including off-premises trading). The prioritised reviews were conducted by leveraging resources available from the firm's first and second lines of defence and provided assurances to management with respect to its ability to conduct business efficiently and effectively during the COVID-19 disruptions. In addition, requests to defer audit reviews were assessed and approved by the Board so as to ensure that they were justified and the corresponding risks arising from any delays in conducting the reviews were properly addressed.

Operational resilience standard 2: Operational risk management

Operational resilience standard 2

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

Intermediaries should establish and maintain effective policies and procedures to ensure the proper management of operational risks to which they are exposed[5]. 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[6].

Suggested techniques and procedures

10. An operational risk management framework may include the following:

(a) the types of operational and regulatory risks posed by potential disruptions and the approach to monitoring and mitigating these risks;

(b) the roles and responsibilities of senior management and other designated staff in developing and implementing risk management policies and procedures; and

(c) the arrangements and measures for ensuring that the intermediary's operational resilience will not be affected by inappropriate processes, inadequate systems or the absence or departure of any staff member[7]. These arrangements and measures include:

---

5 Part VIII of the Internal Control Guidelines.

6 Paragraph VIII(4) of the Internal Control Guidelines.

7 General Principle 3 of the Code of Conduct and paragraph 35(d) of the Appendix to the Internal Control Guidelines.

- regularly reviewing processes and systems and assessing their vulnerability to disruptions;

- regularly reviewing whether any functions are currently carried out by a single staff member or a small group of staff and assessing the disruptive impact of the sudden absence of these staff on the intermediary's business operations; and

- implementing appropriate measures to avoid, mitigate and manage these vulnerabilities and their impact. For example:
  - having backup systems;
  - having multiple staff working on the same team and at different locations; or
  - arranging for support to be provided by group companies or third parties.

Case examples

11. Some firms had the following arrangements to ensure that they could continue to provide services in case of operational failures or the unavailability of systems:

    - having arrangements with one or more brokers so that they could route orders to the exchanges when their own trading systems are not accessible; and

    - having multiple backup data centres to minimise the impact on trading systems caused by malfunction of primary data centres.

12. To cater for situations when office premises are inaccessible, a number of firms provided staff with remote access, commonly through mobile devices or firm-provided laptops, to their internal systems or trading platforms to enable them to carry out their duties off-site.

13. A firm implemented split-team arrangements and then one of its staff contracted COVID-19. As some staff on the same team worked in the office and others worked from home, not all of them were classified as close contacts of the infected staff and required to be placed in mandatory quarantine. As such, the firm was able to continue to provide services to clients.

Lessons learned

14. A firm did not implement split-team arrangements for its trading staff at the outset of the pandemic and all of its traders worked in the same office premises in Hong Kong. When one trader was confirmed positive with COVID-19, the firm had to temporarily suspend its critical trading function as a number of traders were placed in mandatory quarantine. The firm had since set up a backup office in Hong Kong to have staff from the same trading desk work in alternate locations.

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

Operational resilience standard 3
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[8].

Required implementation measures
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.

Suggested techniques and procedures

15. Steps are taken to:

    (a) regularly assess the adequacy and security of the IT infrastructure, software and hardware which are required for ensuring operational resilience. For example, back up and store critical data offline and perform failover and recovery tests;

    (b) prevent and detect the occurrence of errors, omissions or unauthorised insertions, alterations or deletions of, or intrusions into, the intermediary's systems and data; and

    (c) identify cybersecurity risks and implement cyber incident management plans so as to respond to cyber incidents promptly.

Case examples

16. Some firms adopted the following practices to ensure that staff could properly record client's order details when working remotely:

    - installing an IP phone system which supported the recording of calls received and placed by remote-working staff;
    - requiring frontline staff to use only company assigned recorded telephone lines to perform transactions for clients; and
    - requiring trading staff who received orders outside the usual place of business to call back to the firm's telephone recording system to record the orders or record the order details in writing.

---

8 Paragraph IV(2) of the Internal Control Guidelines.

17. A number of firms allowed staff to access their systems and client data remotely. In order to protect these systems and data, some firms:

- required multi-factor authentication and designated usernames and passwords for remote access to the firm's platform;
- required remote access right requests to be approved by line managers and re-certified as part of their semi-annual entitlement review; and
- monitored the use of remote access and disabled remote access rights if staff did not use it in any 30 days.

18. To detect and prevent the leakage of confidential information:

- A firm sample-checked virtual meetings and conference calls made through its computers or mobile devices to ensure sensitive and confidential information was properly handled and due processes were observed when carrying out business activities.
- A firm applied strong encryption of the data hosted on its platform and in emails. In addition, it deployed preventive controls such as blocking outbound emails for non-permanent staff and the transmission of documents classified as secret.
- A firm had policies in place to ensure the proper segregation of corporate and personal data and applications to avoid the transfer of data from one environment to another.
- A firm issued guidelines explaining that its clean desk policy and policy for handling sensitive and confidential information apply to situations where staff are required to work remotely including WFH. To prevent the leakage of data and information, the firm also recommended that traders should perform their duties in separate rooms which are not shared with other parties when WFH or working outside office premises.

19. A number of firms have taken active steps to protect their systems against cyberattacks. For example:

- A firm deployed software to perform system and antivirus checks every time an employee accessed its network remotely.
- Some firms issued additional guidance to staff to remind them of cyber threats and other technology risks associated with remote working.
- A firm closely monitored the impact of the pandemic on the global technology and cyber risk landscape and implemented corresponding controls to address the evolving risks. These included overstretched employees' vulnerability to phishing attacks, greater dependence on remote working IT infrastructure, increased

requests for exceptions to the prohibition of printing at home and use of USB devices to store and transfer information.

Lessons learned

20. A firm failed to properly set up phone recording profiles during a system migration conducted to facilitate WFH arrangements. As a result, some client calls related to order instructions were not recorded.

21. A firm reported a ransomware attack. The back-end server was first infected with a virus and other servers (including trading platforms) were subsequently affected as the firewall system was unable to isolate the compromised server to prevent further malware infections. The business contingency plan was triggered and the firm suspended securities trading activities on its internet and mobile trading platforms, client money withdrawal services and part of its futures trading services. The firm was unable to inform clients of the suspensions since the client contact list stored in the back-end server had become inaccessible. The root causes of the failed response to the incident included the firm's inability to detect and prevent unauthorised system access and promptly isolate the compromised server. To resume its services and rectify system deficiencies, the firm deployed new equipment and rebuilt the servers, strengthened its network security to ensure prompt and efficient responses to malware infections and enhanced its backup arrangements to maintain data tapes in an offline medium.

Operational resilience standard 4: Third-party dependency risk management

Operational resilience standard 4
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
Intermediaries should take appropriate steps to identify, contain and manage third-party dependency risks[9]. 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[10].

9 Part VIII of the Internal Control Guidelines. In particular, effective policies and procedures shall be established and maintained to ensure the proper management of risks to which the intermediary is exposed.

10 Paragraph VIII(4) of the Internal Control Guidelines.

Suggested techniques and procedures

22. Steps are taken to:

    (a) assess how the unavailability of key service providers will affect the intermediary's business operations;

    (b) regularly review reports on systems and controls and test results or other equivalent assessments for service providers and establish processes and benchmarks for monitoring a service provider's ability to deliver services during disruptions; and

    (c) implement appropriate arrangements and measures to avoid, mitigate and manage the impact of service providers' unavailability. For example:

        - clearly set out in the agreements with the service providers the arrangements in case of any disruptions;
        - understand service providers' business continuity plans, including the frequency of testing and reviews; and
        - appoint backup service providers which may be available to assist in the event of the service providers engaged by the firm are unable to continue delivering services.

Case examples

23. When performing due diligence on third-party service providers, some intermediaries paid extra attention to their business continuity plans or arrangements to ensure that they were able to deal with operational disruptions. In particular, a firm partnered with key vendors to design resiliency plans for possible contingencies under different disruption scenarios and establish testing programmes with critical vendors to assess their recovery capabilities.

24. To mitigate the vendor concentration risk, a number of brokers engaged different internet service providers for their primary and backup data centres.

Operational resilience standard 5: Business continuity plan and incident management

Operational resilience standard 5
Intermediaries should have an effective business continuity plan in place to respond to, adapt to and recover from disruptive incidents[11] 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

[11] Paragraph 36 of Appendix to the Internal Control Guidelines.

as well as to prevent their recurrence or mitigate their severity.

Required implementation measures

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.

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.

Case examples

25. Some firms' business contingency plans covered a wide range of scenarios, including disruptions of trading and non-trading systems, inaccessibility of office premises, pandemics, network outages, suspension of power supply, loss of senior management staff and building loss. The approval needed for activating the plans and methods for notifying clients about the activation of the plans were also clearly specified in these plans.

26. Most firms reviewed their business contingency plans periodically. During the COVID-19 pandemic, some firms promptly reviewed their plans to take into account possible operational disruptions due to outbreaks.

27. A number of firms tested their business contingency plans on a regular basis to ensure that the plans could be properly implemented when disruptive events occur. For example:

- A firm tested the relocation to the backup site to ensure that staff would know how to get there, the computers and printers would be correctly configured, working space and facilities on the site would be adequate and its recovery plan (eg, data availability and system performance) would be effective.

- A firm regularly tested its remote access to various systems, including online trading, market making, settlement, financial, accounting and email, through the internet to ensure they functioned properly.

28. Some staff of a firm were classified as close contact of persons infected with COVID-19 and admitted to a quarantine centre. The firm swiftly delivered the necessary equipment such as mobile data SIM cards and stationery to the quarantine centre so that these staff could access the firm's system remotely and carry out key functions as necessary.

Lessons learned

29. Some firms' business continuity plans did not cover possible disruptions brought by an inability to access their office premises. As a result, certain services could not be provided to clients when their office premises became inaccessible.

Remote working

1. Remote working refers to a situation where staff carry out work at a location other than an intermediary's office. It includes relocating staff to their "home offices" (ie, WFH). In general, remote working poses risks because the control and oversight measures designed for use in a traditional office-work environment may not be effective. There are also additional risks which are unique to WFH.

2. The major possible risks associated with remote working (including WFH) discussed in this section are not meant to be exhaustive. Intermediaries should assess the risk profiles of their own remote working arrangements and ensure that all risks are properly identified and addressed.

3. This section sets out the expected regulatory standards for managing and mitigating these major risks. Suggested techniques and procedures are also provided although intermediaries may adopt different techniques and procedures appropriate to their risk profiles in order to comply with the expected regulatory standards. However, they should put in place proper governance and oversight mechanisms which are commensurate with their size and internal organisation to ensure the effectiveness of the techniques and procedures adopted.

Governance

Resources and capacity

4. The risk of insufficient or inappropriately-planned resources (including people, hardware, software, system capacity and connectivity) which may arise from the transition from working in the office to remote working could adversely affect the sound, efficient and effective operations of an intermediary's business. For example, staff may not be provided with the equipment necessary to perform their work efficiently at a remote location or may be unable to access the intermediary's systems remotely due to a slow internet connection.

5. Time-sensitive trading activities, such as market making of listed products where intermediaries are obligated to provide price quotes in a timely manner, require high speed and low-latency trading infrastructure. When inferior networking equipment and software are used and less bandwidth is available at remote locations, an intermediary is exposed to an increased risk of failing to provide price quotes and comply with the requirements of the exchange.

6. Another example is that trade settlement services to some clients may be disrupted under a split-team arrangement when the office has insufficient staff to receive, check and process deposits and withdrawals of physical scrips and cheques.

Expected regulatory standards

Intermediaries should ensure that sufficient resources for the proper performance of work from remote locations are in place[12] before shifting staff to remote working.

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[13]. 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.

In addition, intermediaries should ensure that the IT infrastructure, systems, software, hardware, network capacity and connectivity provided to support efficient remote working[14] are appropriate and adequate.

Suggested techniques and procedures

7. Steps are taken to:

   (a) clearly define functions which could be carried out from remote locations as well as the percentage of staff which could work remotely without hampering the sound, efficient and effective operations of an intermediary's business; and

   (b) regularly review the intermediary's resources and capacity to ensure that they remain adequate and appropriate over time to support remote working, and update the related policies, operational procedures and controls as necessary.

Supervision or control processes

8. The suspension or deferral of compliance reviews may increase due to remote working arrangements, causing delays in identifying compliance issues.

9. The lack of in-person supervision and controls by trading desk supervisors and compliance monitoring staff over the behaviour of trading staff who conduct off-premises trading activities may result in more non-compliant behaviour and hence heighten market misconduct risk.

10. Some controls may lapse due to the inability to remotely access all the documentation necessary to perform a complete compliance review. For example, compliance staff working remotely may be unable to access client account opening documents, which

---

12 Under General Principle 3 of the Code of Conduct, a licensed or registered person should have and employ effectively the resources and procedures which are needed for the proper performance of its business activities.

13 Under Part VII of the Internal Control Guidelines, effective policies and operational procedures and controls in relation to the intermediary's day-to-day business operations shall be established, maintained and compliance therewith ensured.

14 General Principle 3 of the Code of Conduct.

are only available in physical copies and stored in the office, for the purpose of suitability or anti-money laundering compliance clearance. Intermediaries can avoid these control lapses by digitalising their workflow and eliminating physical copies of documents.

11. Other barriers to conducting effective compliance reviews or supervision in a remote working environment may include the absence of face-to-face interaction which may adversely affect the quality of reviews as the body language of the staff involved cannot be assessed. In addition, managers' coaching or supervision of new or less-experienced compliance staff may be less effective due to the lack of physical interaction.

Expected regulatory standards

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[15] in remote working environments, including providing proper training to staff[16] 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[17] in remote working environments.

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.

Intermediaries should ensure that staff performing the compliance function in remote working environments establish, maintain and enforce effective compliance procedures[18], 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.

Suggested techniques and procedures

12. Steps are taken to ensure that:

    (a) the required logistical and technological support is available for the intermediary to implement effective supervision and control processes. For example, firms implement or accelerate the digitalisation of their workflows and eliminate physical copies of documents; and

    (b) additional human and technology resources, including external consultants, are deployed as necessary.

---

15 Part V of the Internal Control Guidelines.

16 Part III(3) of the Internal Control Guidelines.

17 Parts V(2) and V(3) of the Internal Control Guidelines.

18 Part V(4) of the Internal Control Guidelines.

Off-premises trading[19]

13. Intermediaries are exposed to increased control risks when remote-working staff are allowed to conduct off-premises trading. In addition to the lack of in-person supervision and controls by trading desk supervisors and compliance monitoring staff as discussed in paragraph 9 above, other limitations such as less system support in respect of transaction reporting, trade surveillance and suspicious transaction monitoring may also result in more non-compliant behaviour by trading staff.

14. The risks and non-compliant behaviour related to off-premises trading activities may include:

    (a) orders received by remote-working staff through the telephone are not recorded by the telephone recording system used in the office. As a result, the audit trail for the order instructions and order receiving times may be insufficient to support effective trade surveillance or to resolve trade disputes;

    (b) orders are relayed by remote-working staff to other staff in the office for execution due to a lack of remote access to the intermediary's trading system, resulting in delays in executing orders; and

    (c) remote-working staff cannot gain access to necessary information which is only accessible from the office to:

        - evaluate the market situation and determine the best execution strategy for obtaining the best available terms for clients; and

        - determine the amount of trading profit to be disclosed to the client prior to or at the point of entering into a back-to-back transaction concerning an investment product.

15. Any intentional or reckless use of unmonitored or unencrypted communication applications for sharing confidential trading information by staff who conduct off-premises trading activities may go undetected, increasing the risks of trading malpractice and market misconduct.

Expected regulatory standards

Before allowing staff to conduct any off-premises trading activities[20], 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[21].

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

19 This refers to the situation where staff conduct trading activities out of an intermediary's office.

20 Registered institutions should discuss with the HKMA before implementing off-premises trading as a general practice.

21 Part VII of the Internal Control Guidelines.

Expected regulatory standards

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[22]. 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.

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[23].

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[24].

Independent compliance or audit functions, in close coordination with senior management, business operations, risk management and other relevant control functions[25], 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.

Suggested techniques and procedures

16. An oversight mechanism which includes the following is implemented:

(a) more frequent reviews and enhanced supervisory measures for off-premises trading activities such as approval by designated management personnel, and monitoring of off-premises trading activities by means of a set of breach and incident reporting tools and reporting metrics which will prompt escalation of

---

22 Paragraph 3.9 of the Code of Conduct, Paragraph VII(6) of the Internal Control Guidelines and Paragraph 2 of the Circular to Intermediaries on Extended deadlines for implementation of regulatory expectations and reminder of order recording requirements under the COVID-19 pandemic issued on 31 March 2020.

23 Paragraphs 3.1 and 3.2 of the Code of Conduct.

24 Paragraph 8.3 Part A(a)(ii) of the Code of Conduct.

25 Parts V and VI of the Internal Control Guidelines.

material risks to senior management; and

(b) enhanced surveillance capabilities, including the use of effective trade and communication surveillance tools in the off-premises trading environment, to identify potential issues or trends which need to be addressed.

Outsourcing and third-party arrangements

17. Failure by key third parties to provide the services or products required by an intermediary to support remote working arrangements is an inherent risk of remote working. This risk is exacerbated when the third parties and the technologies and expertise provided by them are relied upon by the intermediary's remote-working staff to perform core business or operational functions[26].

18. For example, risks from outsourcing and third-party arrangements may arise when a third-party broker cannot provide execution services to the intermediary because its operational requirements are incompatible with the intermediary's remote working arrangements, or when a third-party broker fails to execute a business continuity plan during a disruptive event. The intermediary may be unable to execute transactions for itself or its clients as a result.

Expected regulatory standards

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[27].

Suggested techniques and procedures

19. The following measures are implemented for outsourcing and key third-party arrangements:

(a) Business continuity and resilience risks

- Conduct regular assessments of key third-parties' capabilities to effectively execute business continuity plans and provide the required services to the intermediary in the event of a disruption, with periodic testing of backup facilities;

- Where appropriate, conduct a review of the financial status of key third parties to ensure they are not at risk of becoming insolvent due to a disruptive event; and

---

26 For example, the execution of orders as well as the clearing and settlement of transactions.

27 General Principle 3 of the Code of Conduct under which intermediaries are required to employ effectively, among others, the resources which are needed for the proper performance of their business activities. The resources include the services provided to them by their key third parties.

- Regularly review key third parties' strategies for responding to disruptive events to assess their IT capabilities to ensure they can continue to provide the required services in situations where remote working has to be adopted.

(b) Cybersecurity and information security risks

- Conduct regular reviews of the potential cybersecurity and information security implications of relying on key third parties to perform business or operational functions, taking into account their strategies for responding to disruptive events so as to ensure that the cybersecurity and information security risks are adequately addressed in a remote working environment.

(c) Third parties subcontractors' risks

- Conduct regular reviews of the list of key third parties and their service agreements to identify and confirm the sub-contractors they rely upon for providing services or products required by the intermediary;
- Regularly assess key third parties' risk mitigating measures to ensure that they can adequately address the potential impact of business disruptions on their sub-contractors; and
- Conduct regular assessments of key third parties and their sub-contractors to identify if new risks exist and are properly managed.

Information security

20. The risk of leakage of client information and other confidential information is increased in a remote working environment because remote-working staff may:

(a) bring hard copies of documents outside the office;

(b) dispose of document print-outs outside the office;

(c) forward electronic copies of documents to personal devices;

(d) remote print or screen print documents on the intermediary's systems;

(e) use removable drives for data storage; or

(f) share documents and information through personal emails or unsecure cloud file sharing.

Expected regulatory standards

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)[28] in a remote working environment. Intermediaries should also ensure that their operating and information management systems are secure and adequately controlled for remote working[29].

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

Suggested techniques and procedures

21. Steps are taken to:

    (a) provide clear guidance to staff on how to protect the confidentiality of information when working remotely. For example, find private spaces for conducting phone and video calls and not bring confidential documents in physical form outside the office but rather access them by secure remote access; and

    (b) promote staff's awareness of their obligation to uphold the privacy and secrecy of client information and other confidential information through regular training and staff attestation of understanding of and compliance with related policies and procedures.

Cybersecurity

22. Intermediaries are exposed to a range of cybersecurity risks resulting from IT system attacks (eg, malware and ransomware attacks), which could adversely affect the sound, efficient and effective operations of an intermediary's business.

23. The use of internet connection and personal devices for remote working aggravates this risk. For example, an intermediary's proprietary, confidential or client data can be intercepted over the internet if staff are allowed to carry out their work using personal computers or mobile devices which are not secure beyond a simple antivirus programme or firewall.

Expected regulatory standards

Intermediaries should establish appropriate measures to manage and mitigate the cybersecurity risks associated with remote working arrangements[30], 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.

---

28 Part IV(5) of the Internal Control Guidelines.

29 Part IV(2) of the Internal Control Guidelines.

30 Paragraph 4.3 of the Code of Conduct and Circular to Licensed Corporations on Management of Cybersecurity Risks associated with Remote Office Arrangements issued on 29 April 2020.

Suggested techniques and procedures

24. Steps are taken to:

    (a) develop and maintain a cybersecurity incident management plan which covers security incidents caused by remote working arrangements; and

    (b) provide regular training to remote-working staff on the prevention of cyber events.

Record keeping

25. Remote working arrangements increase the risk of delay, impairment and fragmentation of certain types of records required to be kept pursuant to regulatory requirements. In particular, when the activities conducted by remote-working staff are not captured in the records and documents generated by the centralised systems, and records and documents held by remote-working staff are not sent back to the licensed corporations' approved office premises, the licensed corporation may be in breach of the requirement of section 130 of the Securities and Futures Ordinance (SFO).

Expected regulatory standards

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.

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 SFO, 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[31].

Notification obligation

26. Intermediaries are required to notify the SFC and where applicable the HKMA of significant changes in their business plans covering internal controls, organisational structures, contingency plans and related matters, including shifting staff to remote working where it constitutes a material change in their business plans. Intermediaries may overlook this notification requirement when a remote working arrangement is deployed for a short period of time.

Expected regulatory standards

Intermediaries should implement measures to promptly notify the SFC and where applicable the HKMA of the implementation of remote working arrangements which

[31] Answer to question 8 of Frequently Asked Questions on Licensing related matters in light of the COVID-19 pandemic.

Expected regulatory standards

constitute significant changes in their business plans and any significant changes in these arrangements[32].

Working-from-home (WFH) arrangements

27. WFH creates additional risks which are unique to a home-office environment.

28. Since family members, neighbours and friends may frequently visit the home office, there is a heightened risk of potential unlawful disclosure of client information, proprietary information or other confidential information by WFH staff to these parties.

29. WFH staff also face a higher risk of network instability because residential networking equipment and software (eg, WIFI routers) may not have the same depth or breadth of features as the equipment and software installed in the intermediary's office for commercial use. Residential networks may also be exposed to a wider range of threats, such as malware.

Expected regulatory standards

Intermediaries should establish and maintain adequate internal controls and operational capabilities which are necessary to mitigate any additional risks unique to[33] WFH arrangements.

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.

Intermediaries should provide specific training[34] to WFH staff on the policies and procedures for protecting the secrecy of confidential information in a home office environment.

Suggested techniques and procedures

30. Steps are taken to:

    (a) permit WFH staff to access client information, proprietary information and other confidential information only through secure firm-provided devices and systems; and

---

32 Sections 135(3) and 135(4) of the SFO. Under paragraph 9 of Part 1 and paragraph 9 of Part 2 of Schedule 3 to the Securities and Futures (Licensing and Registration)(Information) Rules, notification is required to be made by a licensed corporation and registered institution if there are significant changes in the business plan of the licensed corporation and registered institution covering internal controls, organisational structure, contingency plans and related matters.

33 General Principle 3 of the Code of Conduct.

34 Part III(3) of the Internal Control Guidelines.

(b) obtain from WFH staff periodic attestations of the understanding of and compliance with the policies and procedures for protecting secrecy of confidential information and provide regular refresher training to them.