# Regulatory standards and measures on operational resilience and remote working arrangements of the Securities and Futures Commission (“SFC”)

mazars

# In brief

**As a hybrid mode of working is likely to be the new normal in the financial industry even after the pandemic is under control, licensed corporations and registered institutions (collectively "intermediaries") should be more vigilant to operational resilience and the risks associated with remote working to better sustain their businesses.**

**To supplement existing guidance for intermediaries to adopt, the Hong Kong Securities and Futures Commission ("SFC") recently published a report setting out five operational resilience standards and required implementation measures. The report discusses expected measures to manage the major possible risks of remote working arrangements, including working from home.**

**This publication outlines the key regulatory requirements from the SFC report. Mazars offers a wide range of financial advisory services to assist you in achieving compliance with the rules and regulations relevant to you.**

## The five operational resilience standards and their required implementation measures are summarised as follows:

### A. Governance

***Establishing an effective governance framework:*** senior management is responsible for establishing operational resilience objectives, developing and implementing the necessary arrangements and measures, which should be monitored by designated staff on an ongoing basis.

### B. Operational risk management

***Establishing an effective operational risk management framework:*** the framework should assess the potential impact of disruptions on operations, compliance matters and manage the involved risks. The operational risk management framework should also elaborate on the following areas,

i. types of operational and regulatory risks and their respective mitigation approaches

ii. roles and responsibilities of senior management and designated staff

iii.backup arrangement and measures in the lack of resources.

### C. Information and communication technology (“ICT”) including cybersecurity

***Building and operating resilient ICT systems in a secure environment:*** it is crucial to protect the confidential data and information in possession, and manage cybersecurity risks continuously. Relevant policies and procedures should cover regular IT assessments, preventive measures to avoid system malfunction and cyber incident management plans.

### D. Third-party dependency risk management

***Identifying and managing the dependencies on key third parties:*** reviews should be conducted to evaluate how the unavailability of key service providers will affect business operations and how well are they in delivering services during disruptions. Meanwhile, intermediaries should communicate with third parties regarding the business continuity arrangements, and appoint backup service providers.

### E. Business continuity plan and incident management

***Establishing an effective business continuity plan:*** it aims to respond to, adapt to and recover from disruptive incidents. The plan should be reviewed at least annually to address various scenarios and set out procedures, such as the process of identifying root cause, determining appropriate actions, escalating and reporting, preventing similar incidents, and communicating with stakeholders.

# Remote working – key areas of focus

## The expected regulatory standards for managing and mitigating remote working risks are summarised as follows:

### I. Before allowing or shifting staff to remote working

Intermediaries should establish and maintain effective policies and procedures, oversight mechanism, systems and controls, to ensure the following expected regulatory standards are met:

**Governance**

- Sufficient resources for the proper performance of work remotely
- Appropriate minimum number of on-site staff presence for high-risk functions
- Appropriate and adequate IT infrastructure services for support purposes

**Off-premises trading**

- Full integrity of activities and compliant with all regulatory requirements

**Outsourcing and third-party arrangements**

- Proper selection and appointment of key third parties

**Information security**

- Appropriate and effective data security preventive measures and controls
- Secure and controlled operating and information management systems

**Cybersecurity**

- Appropriate cybersecurity risk mitigation measures

**Record keeping**

- Proper procedures for staff to send back certain requisite records and documents to approved premises as soon as practicable

**Working-from-home (“WFH”) arrangements**

- Adequate internal controls and operational capabilities for risks mitigation

# Remote working – key areas of focus (Cont'd)

## II. When staff are allowed to remote working

Intermediaries should implement ongoing controls, to ensure the following expected regulatory standards are met:

### Governance

- Regular reviews and updates of relevant policies, procedures and controls
- Effective supervision and control processes to ensure staff's compliance
- Adequate compensating controls for any suspended controls
- Stringent controls performed by remote-working compliance staff

### Off-premises trading

- Recorded phone lines are used to receive agency orders*
- Appropriate measures to receive client orders through instant messaging
- Available access to trading systems for prompt execution of client orders
- Available system access for information to determine the trading profit amount and disclose to clients before or during back-to-back transactions
- Proactive compliance oversight by independent compliance or audit teams

### Outsourcing and third-party arrangements

- Regular reviews on key third parties to identify their (i) business continuity and resilience risks, (ii) cybersecurity and information security risks, (iii) third parties subcontractors' risks

### Information security

- Strict enforcement of a need-to-know basis on remote access to client information and other confidential information

### Cybersecurity

- Regular training to remote-working staff on the prevention of cyber events

### Record keeping

- Complete records and documents of system activities are maintained

### Notification obligation

- Prompt notification to the regulators of any significant impacts or changes with regard to WFH arrangements

### WFH arrangements

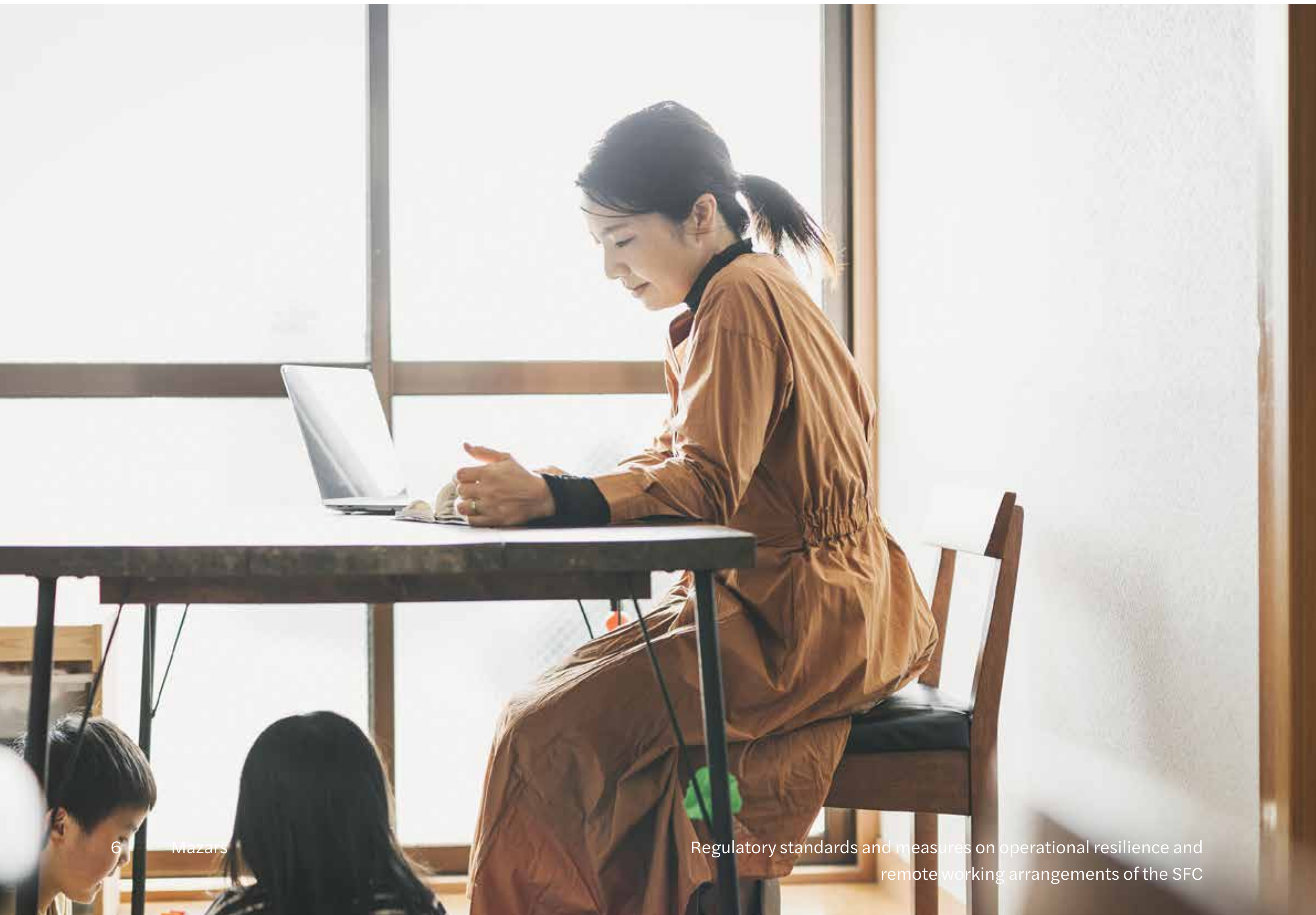
- Strict enforcement of a need-to-know basis on WFH remote access to client information and other confidential information
- Specific training to WFH staff on confidential information secrecy protection in a home office environment

*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.

# How can Mazars help?

**At Mazars, we have extensive experience working with the diversity of financial services players. We assist major financial institutions including brokerage houses, asset managers, investment and corporate banks, retail and private banks, central banks, and national regulators in dealing with business and regulatory issues with impacts, domestic and international.**

**Mazars is here to assist you in complying with the operational resilience standards and required implementation measures, as well as the expected regulatory standards with regard to remote working. Depending on the scope, coverage and specifics of your needs, our services would typically involve one or more of the following:**



# How can Mazars help?

## A. Regulatory reviews and advice

I. Review and provide compliance advisory on your firm's

- policies and procedures,
- processes and controls,
- business continuity plans, and/or
- governance and supervision.

II. Provide observations and recommendations to assist you in complying with the operational resilience and remote working arrangements.

III. Review related documentation and records to ensure compliance.

## B. Design and implementation of policies and procedures

I. Provide advice/ assistance in designing and implementing enhancements to the compliance manual, including governance framework, as well as policies, procedures and controls relevant to operational resilience and remote working arrangements.

II. Provide advice/ assistance in designing and reviewing related risk framework and risk matrix.

## C. Training and insights

I. Provide training and education for staff, the board, senior management and compliance team to facilitate remote working.

II. Provide ongoing insights into how peer firms are dealing with the regulatory requirements and any common challenges encountered along the way.

**We also take on special projects and ad-hoc mandates. We are flexible in our approach and offerings. Please feel free to contact us with any enquiries.**

# Contacts

## Mazars Consulting (HK) Limited

42nd Floor, Central Plaza
18 Harbour Road
Wanchai
Hong Kong

Tel: (+852) 2909 5555
Fax: (+852) 2810 0032
Email: info@mazars.hk

**Ernest Yiu**
Managing Director - financial services
(+852) 2909 5585
ernest.yiu@mazars.hk

**Pierre Latrobe**
Executive Director - financial services
(+852) 2909 5572
pierre.latrobe@mazars.hk

Mazars is an internationally integrated partnership, specialising in audit, accountancy, advisory, tax and legal services*. Operating in over 90 countries and territories around the world, we draw on the expertise of more than 42,000 professionals – 26,000+ in Mazars' integrated partnership and 16,000+ via the Mazars North America Alliance – to assist clients of all sizes at every stage in their development.

*where permitted under applicable country laws

**Follow us**

| | |
|---|---|
| LinkedIn: | www.linkedin.com/company/mazars-in-hong-kong |
| Facebook: | www.facebook.com/mazarsHK |
| Instagram: | www.instagram.com/mazarshongkong/ |
| Twitter: | www.twitter.com/MazarsHK |

**www.mazars.hk**

mazars