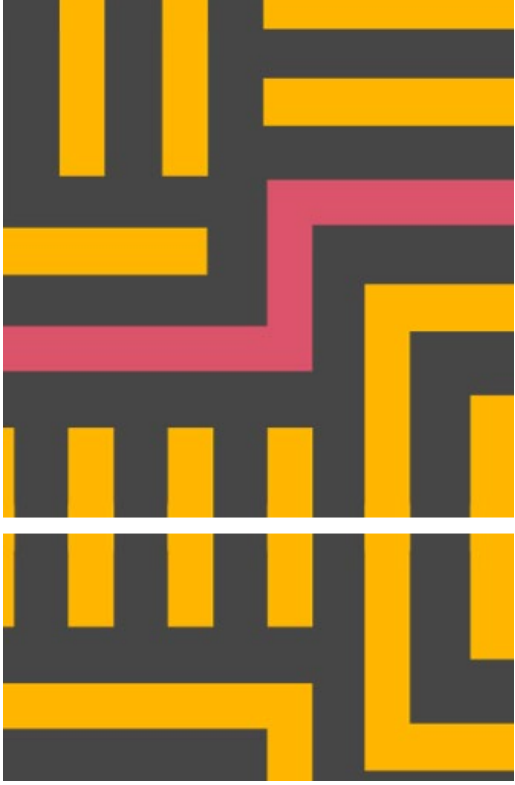
[Respond to COVID-19] Asset management firms staying connected and operating remotely



In brief

The sudden outbreak of novel coronavirus (COVID-19) has challenged the business community's reaction and response to this unexpected situation. With the announcement of a series of measures such as holiday extension, epidemic disclosure, and country-wide quarantine, many organizations have to operate it business remotely and connect virtually (hereinafter referred to as remote office). This undoubtedly is putting the companies' Business Continuity Plan (BCP) into test. As compared to natural disaster scenarios such as fires and typhoon, the epidemic scenario does not destroy the IT infrastructure, but heavily impact the company's daily operations instead.

Many asset management firms have generally adopted a staggered strategy to allow a small number of employees to work on-site rotationally, with the reminder employees to work remotely at home, striving to maintain normal operation of the businesses and market. In a short period of time, asset management companies have completed the test of remote working and stabilized business operations, which proves the efficiency of the industry.

This paper focuses on the business challenges due to remote working and explores how asset management firms are connecting the various aspects in relation to compliance, security, and efficiency to achieve an agile and effective operational business process.

In detail

1. Controls over investment transactions

Investment transactions are the core business of asset management institutions. Here are some of the risks to consider under the current situation:

- **Security threats on remote access to the system** – Security threats such as insufficient complexities of remote access login password and failure to enable the remote logging function increase the cybersecurity risk.
- **Terminal security threats** - Using terminal devices in a relatively loosely controlled environment at home may compromise the company's IT security policy. There is a heightened risk caused by laptops not being upgraded in a timely manner, or by employees using unsecured home computers to connect to the company's network.
- **Internal and external network segregation security vulnerabilities** - Remote access to the business internal network may compromise the segregation of internal and external networks, which could result in potential network or server attack. Employees' portable computers accessing the internet while remotely accessing the company's intranet may cause additional cybersecurity risks due to inadequate internal and external network segregation.

pwc

- **Access management risk** - The same level of remote access permissions should not simply be granted to everyone. Proper remote access management can prevent security threats caused by excessive remote access rights granted to staff.
- **Insufficient operating efficiency** – Additional monitoring on the operating efficiency of remote system access is required, such as the speed and stability of the system as a result of overloaded operations.
- **Personnel qualifications** - There may be situations where employees are authorized to access the system remotely. Under the current circumstances, it is important to ensure that employees who are authorized to access the core system are qualified. In particular, employees placing orders through the investment trading system on behalf of the portfolio managers must hold the necessary qualifications (e.g. relevant SFC licensing requirements).
- **Insufficient behavior monitoring** - To prevent the company's internal control failure, companies need to ensure the traders' mobile communication tools are being monitor effectively during trading hours.
- **Employees' identities** – Controls must be in place to ensure that the user accounts of the investment trading system are used by the designated employees, to prevent the risk of account sharing.
- **Sensitive information leakage** – Controls should be implemented to prevent sensitive data such as trading instructions and positions stored in laptops from being stolen, or information leakage caused by unencrypted data transmission or unprotected local storage.

Areas to consider in relation to remote trading include:

- **Supervision report** - The need for a remote connection to the core business system needs to be reported to the compliance department.
- **Remote access method** – The channel should be secured and reliable for accessing the company's network, e.g. via VPN, setting up of two-factor authentication, etc. The remote access account should be held by individuals and should not be shared. The company should centralise the terminals that can access the company's VPN, and ensure proper security configuration to prevent illegal access.
- **Telephone line and network bandwidth** – procedures should be taken to guarantee the company's network capacity and strengthen capacity monitoring procedures. Companies should take measures to expand the capacity once it is found to be above the threshold.
- **Video devices** – equip traders with video camera equipment to monitor their investment behaviours where appropriate, taking personal privacy into consideration.
- **Screen recording software** – Ensure the quality of screen recording, which should be clear and identifiable; use the company's centralised screen recording tools and storage method as much as possible; if the company's bandwidth is limited for file transfer, public cloud that supports encrypted transmission and storage can be considered.
- **Storage capacity for audio and video files** - With remote working, the number, and size of audio and video files may increase significantly. The capacity of the storage device should be properly estimated and prepared.
- **Portable computers** - Company's portable computers should be properly configured, such as prohibiting the installation of software that does not meet the corporate requirements, revoking permissions of the super administrator rights of the portable computer, incorporating portable computers into the company's domain control environment, prohibiting the use of USBs and other additional storage devices, and enforcing full disk encryption requirements, etc.
- **Audit log** – Audit logs should be maintained to accurately and completely capture the correspondences of investment transaction records, operators, recording systems, audio, and video records.
- **Undertaking letter** - Consider requesting personnel with remote access to sign an undertaking letter to ensure compliance with professional ethics and regulations.
- **After the epidemic is over** - Disable the system's remote access and temporary authorization in time.

2. *Operating off-site*

Although a large number of in-person services have been reduced due to the epidemic, the BCP of these business functions should still be considered. If customers, especially institutional clients or high net-worth clients, put forward business requirements remotely, here are some of the risks to be considered:

- **Compliance risks** - Recording of sales processes under remote working, and after-hours transaction management control.
- **Special business risks** - Alternative solutions for document handling such as discretionary account termination.
- **Archiving risk** - Materials are scattered, and there is an increased risk caused by untimely archiving.
- **Risk of customer information leakage** - Risk of personal information leakage caused by the theft of customer information through remote portable computer terminals.

Areas to consider in relation to remote direct selling include:

- **On-line transfer solutions** - As robo-advisory are becoming increasingly popular, asset managers can facilitate online sales and remote signing of the electronic agreement.
- **Electronic filing** - It stores business documents in a timely manner and prevents loss of documents caused by working offsite.
- **Customer data management and control** - Asset management companies should strengthen its access controls to the customer relationship management system and the operations system, in particular for employees that can access the customers' personal information via portable devices.

3. *Controls over co-working space*

As compared to a normal office environment, remote working has a greater impact on communication efficiency and effectiveness. As compared to other general organisations, asset management institutions' remote working environment has two distinct characteristics:

i. While a large number of tasks are time-sensitive, and the capital market is changing rapidly, investment decisions must be made in a timely manner. Fund information (e.g. net asset value) may need to be disclosed on a daily basis, which requires close coordination among clearing agents, fund administrators, and custodians, etc.

ii. Day-to-day operations of asset management companies involve the handling of private or sensitive information such as customer data, product information, positions, etc., hence, data privacy and confidentiality are critical.

The following risks are to be considered in a co-working space:

- **Late disclosure** - The epidemic causes a reduction in operating efficiency, and in extreme cases it may cause a fund manager fail to disclose the fund information (e.g. net asset value) in a timely manner as required by the regulations.
- **Confidentiality risks** - If public conference platform software is used that involves the exchange of confidential information, there is a potential risk that private data or trade secrets may be leaked.
- **Lack of approval evidence** - Operational risks caused by incomplete approval evidence under a remote working environment.
- **Lack of support from third-party service providers** - For example, reconciliation efficiency may be lowered due to insufficient staffing of the fund administrator, customer redemption requests may not be handled by the distributor in a timely manner, and system failure may not be resolved quickly due to inadequate support by the IT vendor.

Areas that need to be considered under a co-working space include:

- **Contact tree** - The epidemic affects every employee. The company needs to establish a contact tree that includes everyone in the company as soon as possible. It should update employee's health status on a regular basis, provide instant feedback to problems encountered by remote offices of various business departments, and ensure that important information can be disseminated to staff or escalated to management as soon as possible.
- **External contact mechanism** - In addition to the internal situation of the company, it is necessary to obtain external communication updates quickly. The company needs to designate responsible person to obtain updates from government departments and regulatory authorities in a timely manner, monitor real-time public information, establish a communication channel with external service providers (custodian, distributors, IT vendors), update contact information, and evaluate the emergency response of counterparties.

- **Conferencing software** – There are multiple software available for company employees to conduct web-based conferences. The company should make full use of remote conference software to hold meetings among employees in this exceptional situation. When hosting an important or confidential meeting, employees should select a professional conference system that is deployed by the company.
- **Cloud security** - Remote office will increase the need for data storage and exchange, such as upload or store the recordings. If cloud services are needed, the company may temporarily procure cloud solutions that support encrypted data transmission and storage to avoid security risks.
- **Approval of office automation software** - Remote working restricts written approval. The company can follow the existing electronic approval process and utilise an automatic workflow system for approval of different matters. Requests on changing permissions or opening additional ports to facilitate remote working should be carefully assessed.
- **Office collaboration software**. The company can utilise collaborative tools to collaborate documents and perform version control remotely. Avoid transmitting and storing files that involve trade secrets or undisclosed information using public software.

Let's talk

What are your overall assessment of your emergency plan and implementation when it comes to operating remotely and staying connected? If you want to know more about the above risk points and solutions, please contact us.

Marie-Anne Kong
PwC Hong Kong Asset and Wealth Management Leader
Phone: +852 2289 2707
Email: marie-anne.kong@hk.pwc.com

Jane Xue
PwC China Asset and Wealth Management Leader
Phone: +86 (21) 2323 3277
Email: jane.xue@cn.pwc.com

Jenny Yip
Director, Risk Assurance
PwC Hong Kong
Phone: +852 2289 1968
Email: jenny.py.yip@hk.pwc.com

Aileen Wang
Partner, Risk and Control Services
PwC China
Phone: +86 (21) 2323 6655
Email: aileen.wang@cn.pwc.com