RISK MANAGEMENT AND OPERATIONAL RESILIENCE IN A REMOTE WORKING ENVIRONMENT

Issued jointly by the Monetary Authority of Singapore and The Association of Banks in Singapore

March 2021

CONTENTS

A. INTRODUCTION

Background

The COVID-19 global health crisis, and the attendant public health measures implemented by governments to mitigate human-to-human transmissions, resulted in businesses around the world having to adopt work-from-home (WFH) arrangements on a scale and at a speed that was unprecedented. In Singapore, the proportion of staff of financial institutions (FIs) who were working from home was 85% during the Circuit Breaker[1] period.

FIs in Singapore benefited from their earlier investments in digitalising business processes, customer touchpoints and delivery channels. The lessons learnt from past industry-wide business continuity exercises also put FIs in good stead to manage the sudden shifts in staff's work arrangements. These prior efforts have allowed FIs to remain open during the pandemic to support the needs of individuals and businesses. In addition, The Association of Banks in Singapore (ABS) set up a Return to Onsite Operations Taskforce (ROOT) to facilitate the sharing of good practices among members, and coordinate responses to the COVID-19 situation. While some FIs faced initial challenges of equipping staff with adequate tools for working effectively at home, they have adapted well over time.

At the time of writing, many parts of the world are experiencing resurgences of COVID-19 infections, and the emergence of more contagious variants of the virus. Several countries, including Singapore, have started their national vaccination programmes.

However, it is foreseeable that significant WFH (or remote working, more generally) arrangements, and a hybrid mix of remote working and work-in-office (WIO) arrangements, will likely continue until the global pandemic is brought under control.

There is an increasing recognition by businesses of the need for their operations to be pandemic-resilient in the longer term, beyond COVID-19, in which remote and hybrid work arrangements will play a role. Some FIs have already publicly announced their longer term plans to offer their staff hybrid work arrangements in the "new normal". This is partly due to the need to re-think the available capacity in the office as FIs re-design workspaces to maintain safe distancing between staff, or "pandemic-proof" their offices, for the current and future pandemics. This is partly also in response to the expressed desire of staff to have the flexibility to choose where they work.

[1] The Circuit Breaker is an elevated set of safe distancing measures implemented in Singapore from 7 April to 1 June 2020 to break the trend of increasing local transmission of COVID-19. *(https://www.moh.gov.sg/news-highlights/details/circuit-breaker-to-minimise-further-spread-of-covid-19)*

Remote working risks

Remote working requires changes to policies and operational processes, some of which could lead to new risks and risk management challenges (hereafter “remote working risks”).

ABS ROOT members have generally not observed any significant increase in operational, fraud and cyber risks incidents because of remote working in 2020, since staff transitioned from WIO to remote working, as compared to the prior year.

However, given that large-scale ongoing remote working is a relatively recent development, the associated risks may only emerge over time. The forms that remote working will take, and the resultant risks, will also continue to evolve.

Purpose

In view of the protracted remote working arrangements due to COVID-19, and their likely continued adoption in the longer-term “new normal”, it is important that FIs consider and monitor remote working risks closely so as to take pre-emptive steps to mitigate them.

To this end, the Monetary Authority of Singapore (MAS) and ABS have jointly published this paper to:

(1) Raise awareness of key remote working risks in the financial sector.

(2) Share good practices adopted by FIs to mitigate key remote working risks.

(3) Strongly encourage all FIs to adopt good practices on risk mitigation, set out in this paper, on a risk-proportionate basis according to their risk profiles and business activities.

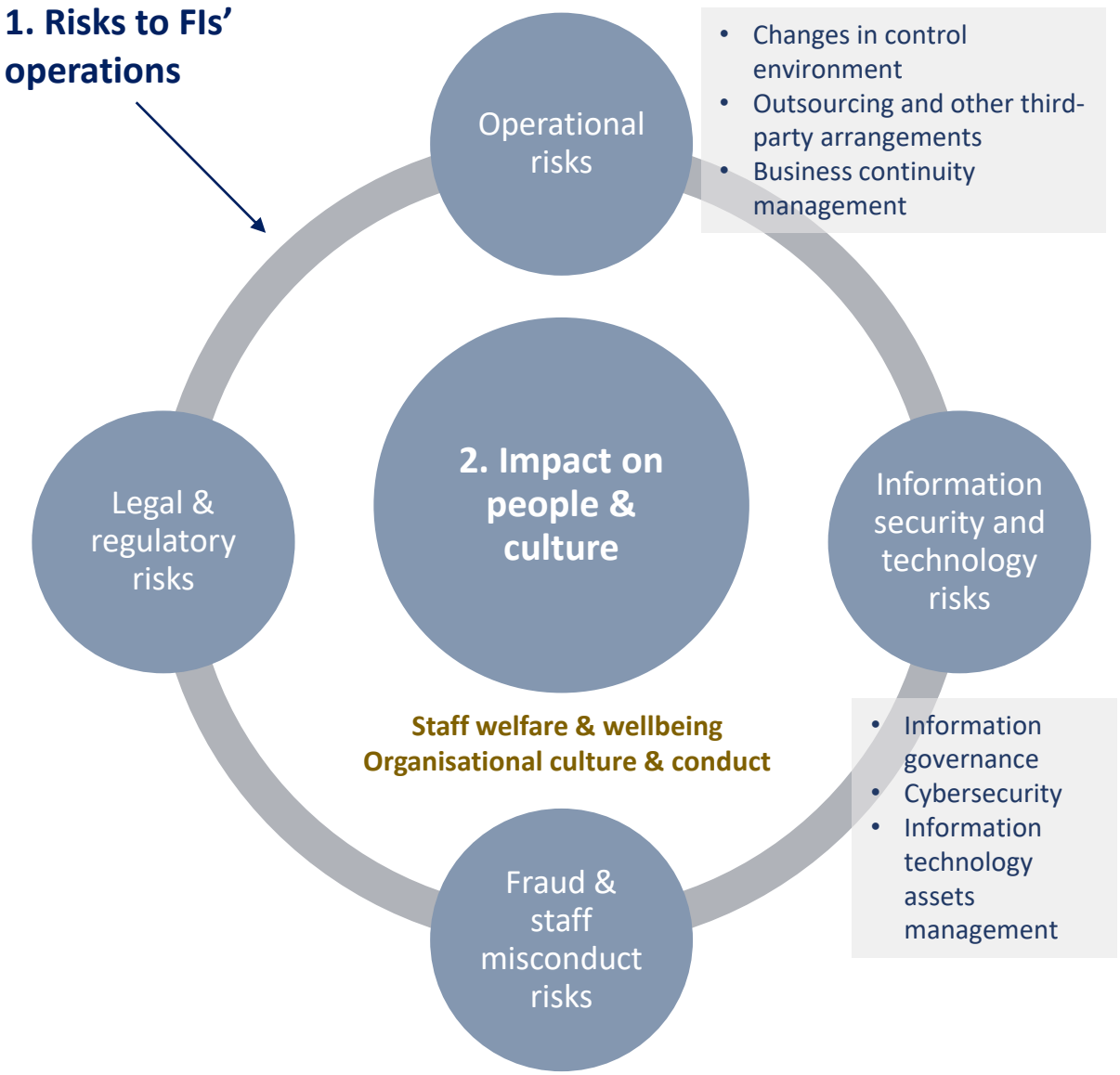
What is Remote Working?*

- When staff are working in locations that are outside FIs’ offices or premises.
- When staff are not connected directly to office networks and applications, but through residential or public broadband networks, or mobile data networks.
- Examples of locations used for remote working include staff’s homes, and other third party premises like hotels and co-working spaces. Locations do not ordinarily include working from FIs’ other offices or branches, such as satellite offices or alternate sites maintained for business continuity management purposes.

* As defined for this paper

Scope and application

The paper covers remote working risks under two main areas - 1. Risks to FIs' operations and 2. Impact on people and culture.



Interactions and interlinkages of risks

While the key remote working risks have been grouped under the above distinct risk categories, there are significant interactions and interlinkages amongst the risks. These risks may also be exacerbated or mitigated by an FI's people and culture. The interactions and interlinkages amongst different risks should be considered when assessing the implications of policy and process changes for remote working.

To illustrate, when staff no longer perform their roles under the direct oversight of supervisors (a change in control environment), coupled with the ability to access confidential information such as customer data (a change in information governance policies and system access controls), staff may have more opportunity to misuse confidential information (an increase in misconduct risks), which could lead to legal and/or regulatory risks if the misconduct occurs.

For each category of remote working risk, the paper sets out:

The contents of this paper, including the examples of mitigating controls, are drawn mainly from the experiences of ABS member banks. However, many of the risks and mitigating controls set out in the paper are also relevant and applicable to non-bank FIs.

Direct vs indirect risks of remote working

The scope of this paper predominantly focuses on the areas of risks where changes, due to remote working, have a direct impact on the risks and risk management challenges faced by FIs (hereafter "direct risks"). However, poorly managed direct risks of remote working could lead to heightened risks in areas that may not be directly impacted by remote working (hereafter "indirect risks").

Examples of indirect risks

(i) *Reputational risk – Significant risk incidents as a result of remote working, such as major processing errors or loss of customer information, could increase reputational risks for the FI or the financial sector as a whole.*

(ii) *Credit risk – Changes in validation processes that are conducted for credit assessment and monitoring purposes, such as replacement of customer site visits (e.g. to ascertain existence of collateral pledged) with customer calls, could affect an FI's ability to identify red flags in customers' circumstances.*

(iii) *Market risk – Issues with internet connectivity or Virtual Private Network (VPN) capacities could affect the ability of dealers and risk managers to react quickly to market volatility and sudden market movements.*

Overview of key risk management actions

The following sets out the key actions that FIs are encouraged to adopt to manage remote working risks:

1 (Changes in control environment): FIs review remote working arrangements to identify risks from changes in control environment and processes. FIs implement compensating controls to manage identified risks within risk appetite statements approved by Board and senior management. FIs adopt robust change management procedures so that staff understand and implement the new processes and controls as intended.

2 (Outsourcing and other third party arrangements): FIs evaluate changes to vendors' risk profiles with remote working, such as by assessing vendors' remote working controls and operational resiliency. FIs implement appropriate safeguards and contingency plans to ensure continuity of services.

3 (Business continuity management): FIs enhance business continuity strategies and procedures to consider the large-scale distribution of its workforce across locations. This includes the implementation of response strategies for recovery team members to resume functions promptly.

4 (Information governance): FIs assess the risks and implications of information loss when determining which activities can be performed remotely. FIs strengthen preventive and detective controls to mitigate these risks.

5 (Cybersecurity): FIs implement controls to ensure that staff's remote working infrastructure, including personal devices, are secured.

6 (Information technology assets management): FIs continue to adopt sound and robust technology risk management practices, to manage hardware and software deployed to facilitate large-scale remote working, including during the pandemic.

7 (Fraud): FIs keep abreast of evolving fraud typologies from remote working and implement appropriate preventive and detective controls. FIs also implement guidelines to identify situations where in-person meetings, site visits and verification against original documents are required.

8 (Staff misconduct): FIs adopt and communicate appropriate incentive structures and consequence management frameworks to drive the right behavior even when staff are working remotely. FIs enhance the monitoring of activities and transactions of staff in high risk roles.

9 (Legal and regulatory): FIs consider legal and regulatory implications when establishing guidance on remote working practices. These include practices on human resource management and the making of legal contracts, especially where transactions and activities involve foreign jurisdictions.

10 (Impact of remote working on people and culture): FIs pay attention to staff's morale and welfare, and provide resources for their emotional and mental support. FIs also explore ways to build strong corporate culture and conduct in a remote or hybrid working environment.

Staying vigilant for evolving risks

This paper was written in the midst of an evolving COVID-19 pandemic situation that has made it necessary for businesses, including FIs, to adopt large-scale remote working.

The paper is, however, intended to apply to remote working more generally beyond the current pandemic, although it has included some references to the challenges faced by FIs in the ongoing crisis. The paper does not cover the initial transitional challenges faced by FIs from WIO to WFH arrangements, which have largely been resolved and are no longer relevant.

The challenges to risk management and operational resilience, due to remote working, and the corresponding mitigating practices set out in this paper are not exhaustive. Amongst others, the ongoing pandemic may present new remote working risks and challenges to FIs which may not have emerged at the time of writing. For the financial sector to remain operationally resilient, and continue to provide a high level of service, FIs need to be alert to the evolving situation and take timely action to address emerging risks.

B. Key risks of remote working to FIs' operations

1. Operational risks

a. Changes in control environment

What has changed?

Large-scale adoption of remote working has changed the overall control environment in which staff perform their roles. Generally, it is more challenging to manage risks effectively in a dispersed remote working situation vis-à-vis an office environment.

Policies and procedures, originally implemented for an office-setting, have been adapted or amended to facilitate remote working.

In summary:

- Tasks that used to be performed under the in-person supervision of managers or in the presence of other colleagues in the office are being, or can potentially be, performed by an individual staff almost anywhere with internet connection.
- Certain systems and confidential information that were previously accessible only from the office are now accessible remotely.
- Assessments that used to rely on physical meetings and site visits are now done through virtual meetings.
- Verifications that were previously performed against original documents are now conducted based on softcopies.

What are the risks?

- FIs not adequately assessing risk implications of allowing specific functions to be performed remotely on a large-scale and over a prolonged period. This could lead to inadequate steps being taken to manage these risks and keep them within FIs' overall risk appetite limits, or to seek approval from FIs' boards and senior management to deviate from these limits *(examples of specific risks and mitigating controls are set out in the rest of Section B of this paper).*
- FIs do not have robust change management procedures to communicate changes to staff, and implement the new processes and their associated controls as intended.

B. Key risks of remote working to FIs' operations

1. Operational risks

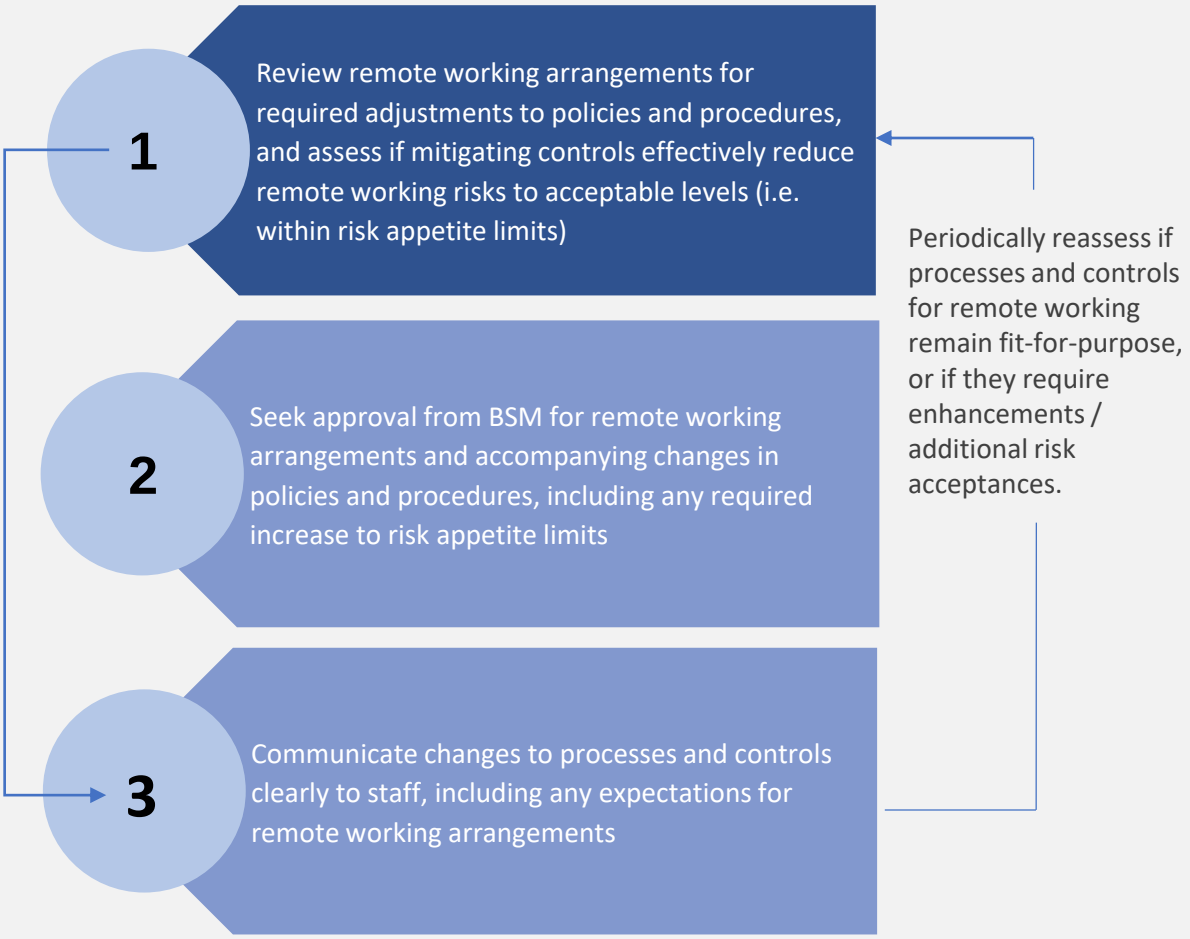
a. Changes in control environment

Key risk management actions

FIs review remote working arrangements to identify risks from changes in control environment and processes. FIs implement compensating controls to manage identified risks within risk appetite statements approved by Board and Senior Management (BSM). FIs adopt robust change management procedures so that staff understand and implement the new processes and controls as intended.

Examples of mitigating controls

Illustrative risk assessment and mitigation process:



Large-scale remote working is a relatively recent phenomenon in the financial sector - aspects of remote working risks may not yet be well-understood, and the effectiveness of corresponding controls have also not been tested over time. Without extensive historical events or data, scenario analysis could be a useful tool for FIs to identify risks and assess the effectiveness of mitigating controls of remote working.

B. Key risks of remote working to FIs' operations

1. Operational risks

a. Changes in control environment

Other examples of general mitigating controls to reduce remote working risks (specific remote working risks and examples of mitigating controls are set out in the rest of Section B of the paper):

Short term measures

- FIs' BSM review and approve risk appetite statements / limits for remote working.
- Develop remote working guidelines, such as factors to determine if a function should be performed remotely (e.g. sensitivity of information handled, impact of error/loss, ability to adequately manage risks), and if a location is suitable for remote working (e.g. risk of leakage of confidential information).
- Implement alternative controls (e.g. conducting video calls instead of physical site visits, reviewing recorded conversations with clients and performing callbacks for more types of activities and transactions, using screen-sharing to perform maker-checker roles).
- Maintain records of changes to work processes and controls for oversight and approval by BSM, and performance of independent reviews (e.g. by internal audit).
- Train supervisors to manage teams remotely (e.g. on how to maintain team engagement), and provide guidance on the identification of suspicious actions or transactions by staff (e.g. through review of activity logs).

Medium to longer term measures

- Review remote working arrangements periodically to assess if controls remain adequate or if they require enhancements / additional risk acceptances (e.g. through scenario analysis). Such reviews should also be subjected to appropriate approval and oversight by BSM.
- Reinstate controls (e.g. in-person meetings, site visits and verification of original documents) to complement alternative controls (e.g. desktop reviews and reliance on softcopy documents), if alternative controls are ineffective for reducing residual risks to acceptable levels within risk appetite limits.
- Digitise hardcopy documents where possible and digitalise workflows and processes, including implementing more system controls, to reduce reliance on manual processes.
- Conduct ongoing assessment of remote working risks and effectiveness of mitigating controls, such as through control self-assessments and internal audits, etc.

B. Key risks of remote working to FIs' operations

1. Operational risks

b. Outsourcing and other third party arrangements

What has changed?

Adoption of remote working by FIs' vendors for outsourcing and other third-party arrangements may change how services are delivered under these arrangements, and potentially vendors' risk profiles. In addition, as staff of both FIs and vendors work remotely, FIs could face challenges in conducting physical audits and site visits.

What are the risks?

- Vendors' infrastructure and controls, including business continuity plans, may not be as robust as the FIs' to allow them to fully manage remote working risks – this translates to heightened risks for FIs, especially if vendors have access to sensitive information, client data or connectivity to the FIs' systems, or provide critical services to FIs.
- Where vendor services were previously provided onsite at FIs' premises (e.g. IT development and support), FIs may no longer be able to closely supervise vendor activities with remote working – this could lead to higher error rates or delays in service delivery.
- With challenges of arranging physical audits and site visits of vendors, FIs may instead conduct alternative procedures, such as desktop or virtual reviews, which generally rely more on vendors' attestations – these are less effective in detecting risk issues, including weaknesses in vendors' infrastructure, controls and operational resiliency.

Key risk management actions

FIs evaluate changes to vendors' risk profiles with remote working, such as by assessing vendors' remote working controls and operational resiliency. FIs implement appropriate safeguards and contingency plans to ensure continuity of services.

B. Key risks of remote working to FIs' operations

1. Operational risks

b. Outsourcing and other third party arrangements

Examples of mitigating controls

Short term measures

- Assess how risk profiles of vendors have changed with their adoption of remote working – evaluate adequacy of vendors' infrastructure, security and operational resiliency, and implement appropriate safeguards, controls and contingency plans.
- Increase monitoring of vendors' performance for timely identification of issues, such as delays or lapses in service delivery standards.
- Increase communications with vendors to understand and resolve performance issues in timely manner.

Medium to longer term measures

- For vendors that allow remote working arrangements, execute or renegotiate contracts with new or existing vendors, requiring them to comply with FIs' remote working and information security policies as conditions for remote service delivery to the extent where it meets the FIs' standards.
- Periodically conduct physical audits, site visits, and joint business continuity and disaster recovery exercises, with vendors to complement desktop reviews or virtual visits. Physical audits and site visits are especially important if vendors manage confidential / customer information or handle tasks requiring strict physical security and access controls (including segregation of teams processing information for different FIs). Virtual reviews may be less effective in assessing vendors' clean desk practices, coverage of security cameras, and processes for production/archival/destruction of FIs' information.
- For annual Business Continuity Planning tests, include tests of key vendors' remote working capabilities and FIs' contingency plans to cover service disruptions of key vendors.

B. Key risks of remote working to FIs' operations

1. Operational risks

c. Business continuity management

What has changed?

FI staff's primary work location has changed from the office to either a remote location, or a hybrid between the two. Accordingly, FIs' considerations for business continuity planning need to extend beyond disruptions within office premises and its infrastructure, and include disruptions involving remote working scenarios.

What are the risks?

With large-scale remote working, effects of disruptions in remote working situations may be compounded if:

- Recovery team members are unable to obtain prompt technical support for their hardware issues, which is typically readily available when WIO.
- Recovery team members' remote working locations are not supported by uninterruptible power supply and/or back-up generators in the event of power outages.
- Recovery team members have no alternative means to connect to the office network when working remotely if there are disruptions in internet or VPN services.

Telco 1 customers hit by major internet outage; working and studying from home affected

SINGAPORE – Telco 1 customers were affected by a major internet outage on Wednesday (April 15), with users in multiple locations across the island complaining of disruptions since the morning.

The disruption lasted for at least nine hours, with Telco 1 announcing that services have been fully restored as of 8.20pm.

Fibre Internet outage hits some Telco 2 users in western, central and eastern Singapore

SINGAPORE – Thousands of Telco 2 fibre broadband users around Singapore were left without Internet access for more than 10 hours on Tuesday (May 12) during a time when subscribers need to work and study from home amid the ongoing Covid-19 outbreak.

Telco 2's disruption, which comes one month after Telco 1's intermittent outage, was still not resolved as at 2.30pm.

According to the Down Detector website, which logs Internet outages, Telco 2 started having problems at around 4.27am, before complaints spiked at 7.27am with 1,185 reports, and again, at 8.42am with 1,432 reports.

B. Key risks of remote working to FIs' operations

1. Operational risks

c. Business continuity management

Key risk management actions

FIs enhance business continuity strategies and procedures to consider the large-scale distribution of its workforce across locations. This includes the implementation of response strategies for recovery team members to resume functions promptly.

Examples of mitigating controls

- Enhance scope of business continuity plans to cover disruptions in remote working situations and include them in scenario testing.
- Make arrangements for staff to resolve hardware issues and access an alternative work location if required.
- Reduce dependencies on any single/critical staff by either cross-training staff or automating processes. If neither of these are viable options, ensure process are adequately documented to facilitate continuity of operations.

B. Key risks of remote working to FIs' operations

2. Information security and technology risks

a. Information governance

What has changed?

To facilitate remote working, FIs may have amended information governance policies to allow staff to access customer and other sensitive information when they are working remotely - staff could previously only access such information within the office premises.

What are the risks?

Allowing staff to access customer and other sensitive information remotely heightens inherent risks of leakage, such as through:

- Shoulder surfing and eavesdropping by family members or strangers.
- Staff printing out sensitive information at home and/or bringing back hard copies of such information for remote working - physical documents could be left lying around unattended and seen by unauthorised parties.
- Staff taking pictures or notes of sensitive information from their laptop screens, or forwarding such sensitive information to personal devices/emails (more easily done without colleagues or supervisors around).
- Staff surfing the internet via the internet service provider (ISP) directly on corporate devices bypassing corporate proxy/internet gateway.

Key risk management actions

FIs assess the risks and implications of information loss when determining which activities can be performed remotely. FIs strengthen preventive and detective controls to mitigate these risks.

B. Key risks of remote working to FIs' operations

2. Information security and technology risks

a. Information governance

Examples of mitigating controls

Preventive measures

- Implement policies and guidelines on locations where staff are permitted to work remotely (e.g. restrictions on working in shared public working spaces such as cafes and hotel lobbies).
- Establish policies, standards and procedures on handling sensitive information remotely.
- Remind staff to safeguard sensitive information.
- Grant remote access to information only on a need-to basis.
- Disable USB ports and Bluetooth to prevent printing and transfer of information.
- Disallow storage of corporate data on personal device, if device not managed by corporate policies.
- Implement Data Loss Protection monitoring tools to prevent and detect data leakage.
- Disable VPN split tunneling and/or enable always-on VPN configuration.

Detective measures

- Monitor user remote access activities to identify any suspicious incidents and trends (e.g. if staff accessed systems during odd times such as after normal working hours, or if staff accessed amount or type of information that is unusual for the role they perform).
- Increase call monitoring and other staff surveillance activities for high risk functions (e.g. trading, investment advisory).
- For business applications, create separate profiles/access groups specifically dedicated to users logging in from outside office locations. This would facilitate more granular monitoring of activities performed by users working remotely, and would allow additional restrictions to apply to sensitive functions.

B. Key risks of remote working to FIs' operations

2. Information security and technology risks
b. Cybersecurity

What has changed?

To enable effective remote working, FIs have allowed remote access to applications and systems, which were previously only accessible from the office. Staff are also conducting work-related discussions remotely on virtual collaboration platforms (e.g. Cisco Webex, Google Meets, Microsoft Teams and Zoom) and personal devices like laptops and handphones.

What are the risks?

- A cyber attack targeting an FI's remote access infrastructure could potentially disrupt its availability and affect remote users.
- Internet set-up in a staff's home or chosen remote working location is generally more difficult to secure than an office-based network.
- Personal devices used to access corporate resources are less secure than corporate-issued devices, if not managed by corporate policies.

Key risk management actions

FIs implement controls to ensure that staff's remote working infrastructure, including personal devices, are secured.

B. Key risks of remote working to FIs' operations

2. Information security and technology risks
b. Cybersecurity

Examples of mitigating controls

- Implement redundancies and reduce single points of failure in remote access infrastructure.
- Increase staff's vigilance of phishing and social engineering scams through regular security awareness programs.
- Implement multi-factor authentication for remote access.
- Ensure that remote access infrastructure is appropriately configured and secured.
- Assess and address risks from use of personal devices to access corporate resources remotely.
- Perform security posture checks on personal devices to ensure they adhere to FIs' IT security requirements (i.e. up-to-date security patching and malware signature) before permitting remote access to the corporate resource.
- Perform penetration testing on remote access infrastructure.
- Provision staff with securely configured mobile router for internet connection if necessary.
- Assess security features of virtual collaboration platforms before use and implement guidelines on safeguards for such platforms (e.g. allowing only registered participants to join in, using a random meeting ID, locking the conference once all the participants have joined, and updating software with the most up-to-date security features).

B. Key risks of remote working to FIs' operations

2. Information security and technology risks

c. Information technology (IT) assets management

What has changed?

FIs may have to supplement existing IT infrastructure, by deploying new hardware and software, to enable effective large-scale remote working. These include new laptops, video-conferencing tools, softphones and other voice recording tools, and other remote desktop applications to allow staff to access more systems or critical applications remotely.

What are the risks?

- New hardware or software introduced to facilitate remote working may not integrate well with existing systems – this could affect the stability and security of FIs' systems environment.
- Remote working increases inherent risks that assets used outside the office may be lost or misplaced – lost / misplaced devices in the wrong hands may allow cyber criminals to impersonate FIs' staff to gain access to FIs' critical systems and sensitive information.

Key risk management actions

FIs continue to adopt sound and robust technology risk management practices, to manage hardware and software deployed to facilitate large-scale remote working, including during the pandemic.

Examples of mitigating controls

- Maintain updated inventory list of all hardware and software assets.
- Conduct comprehensive tests to ensure new hardware and software are compatible with existing software, networks, databases, internet browsers, mobile devices, etc, and if necessary, implement mitigating measures so as not to introduce security vulnerabilities to existing IT infrastructure.
- Remind staff to safeguard IT assets issued to them.
- Ensure that corporate-issued devices used for remote working conform to FIs' security standards and implement hard disk encryption.
- Implement and test disaster recovery plans of the newly implemented hardware and software.

B. Key risks of remote working to FIs' operations

3. Fraud and staff misconduct risks

a. Fraud

What has changed?

Remote working has required changes to certain business practices. For example:

- virtual meetings and calls have replaced face-to-face meetings with customers and site visits.
- soft copies of documents are now accepted in place of original documents.
- digital signatures are used instead of wet-ink signatures.
- FIs are accepting more customer instructions over calls or emails but may face challenges, due to remote working by customers, in performing previously standard call-back checks to confirm customers' instructions.

What are the risks?

- Heightened risks of identity theft with lack of face-to-face contact and verification performed against copies of identity documents instead of originals (copies are more susceptible to forgery and tampering).
- Heightened risks of acting on false customer instructions over calls and emails
  - digital signatures misappropriated by persons with malicious intent
  - customer email domains hacked or spoofed
  - interception and amendment of instructions from customers
  - inability to conduct transaction authentication if customers cannot be reached at registered numbers
- Harder to detect customer fraud without conducting physical site visits - site visits typically conducted as part of credit monitoring procedures to ascertain existence of a customer's business activity, assets or pledged collateral.

Key risk management actions

FIs keep abreast of evolving fraud typologies from remote working and implement appropriate preventive and detective controls. FIs also implement guidelines to identify situations where in-person meetings, site visits and verification against original documents are required.

B. Key risks of remote working to FIs' operations

3. Fraud and staff misconduct risks

a. Fraud

Examples of mitigating controls

Create customer awareness

- Run fraud risk awareness campaigns for customers (e.g. on digital banking platforms, social media, webinars).
- Promote use of digital banking channels for transactions as an alternative to call instructions.
- Encourage use of trusted official sources (e.g. MyInfo) to authenticate identity for onboarding, where possible.

Maintain staff vigilance

- Conduct fraud risk training for staff with tailored guidance for specific functions (e.g. phishing simulation exercises).
- Remind staff to be vigilant for fraud.
- Establish internal escalation procedures to handle suspicious activities and transactions.

Preventive measures

- Use a combination of virtual collaboration tools and/or other technology solutions to mitigate risks from lack of face-to-face meetings (e.g. witness customers signing forms over video calls or through screen-sharing, verify customers' identities and documents submitted electronically using technology authentication tools like AI-based technology, biometrics and known ID authentication features).
- Require corporate customers to register alternate authorised contact numbers, if the corporate customers' staff are working remotely, to facilitate call-backs by FIs to verify/confirm transactions.
- Obtain customers' consent for FI to act on instructions received over calls and emails – call instructions should be received on recorded lines. If FI has no call recording ability, adopt mitigating controls such as requiring customers to confirm the instruction via email after the call.
- Assess if additional verification is required for documents with digital signatures (refer to section on "Legal and regulatory risks") and perform call-backs on recorded lines if needed.
- For transactions based solely on email instructions, set up limits for third-party payments (i.e. payments made to accounts that are not in the customer's name), and define client eligibility criteria for such transactions.

Detective measures

- Strengthen surveillance capabilities, such as by employing data analytics and machine learning to detect fraud, particularly for higher risk functions (e.g. trading, investment advisory).

B. Key risks of remote working to FIs' operations

3. Fraud and staff misconduct risks

b. Staff misconduct

What has changed?

With remote working, staff no longer work under the physical oversight of supervisors or in the physical presence of colleagues.

What are the risks?

Without the physical presence of supervisors and colleagues, some staff may adopt a more lax attitude towards compliance matters or may be emboldened to act inappropriately. FIs may face risks of:

- Staff circumventing work processes and controls (e.g. transmitting confidential information over unauthorised channels to avoid FI's surveillance applications).
- Staff colluding among themselves and/or with other parties for monetary gain; staff may find it easier to forge softcopy documents as opposed to original documents.
- Staff communicating inappropriately with customers/counterparties (e.g. making misleading statements, especially on unrecorded devices).

Key risk management actions

FIs adopt and communicate appropriate incentive structures and consequence management frameworks to drive the right behavior even when staff are working remotely. FIs enhance the monitoring of activities and transactions of staff in high risk roles.

B. Key risks of remote working to FIs' operations

3. Fraud and staff misconduct risks

b. Staff misconduct

Examples of mitigating controls

Preventive measures

- Remind staff to comply with the FI's Code of Conduct, policies and procedures.
- Encourage supervisors to regularly engage staff (e.g. through daily team calls).
- Share lessons learnt from operational lapses and misconduct incidents as reminders.
- Require staff performing higher risks roles, such as traders and investment advisors, to communicate and transact over recordable corporate devices (e.g. corporate mobile phones with softphone applications installed to enable voice recording).

Detective measures

- Conduct periodic reviews of staff remote access activities (especially for staff in higher risk functions such as trading and client investment advisory) to identify any suspicious incidents and trends.
- For staff in higher risk functions, enhance surveillance of staff's communication (both external and internal) and transactions (e.g. by increasing frequency of checks, expanding scope of sample testing for booked trades to ensure they were transacted in accordance with established procedures, and monitoring keystrokes logging).

B. Key risks of remote working to FIs' operations

4. Legal and regulatory risks

What has changed?

- The extent of the adoption of remote working by FIs has materially increased due to the pandemic.
- To facilitate remote working, FIs have accepted certain modes of electronic/digital signing of documents, in place of wet-ink signatures.

What are the risks?

Risks from FIs' staff working remotely

- Risk of complaints and actions by FIs' staff for breach of Employment Act requirements on working hours, rest days, overtime, etc. because working times are less defined.
- Risk of complaints and actions for work-related injuries and illnesses, such as under the Workplace Safety and Health Act as its application to remote working is untested.
- Increased risk of vicarious liability claims from staff's negligence or misconduct while working outside the office as it may be less clear when an act is performed in the course of employment.
- Risk of complaints and actions by clients for breach of confidentiality obligations, Personal Data Protection Act, and other similar requirements on use, disclosure, retention and processing of personal data (e.g. unintended disclosure of customer or other confidential information by a staff or contractor working remotely).
- Risk of non-compliance with laws of other jurisdictions (including employment laws, work safety requirements, confidentiality/personal data protection and privacy laws) applying to staff and contract workers travelling to, or remotely working from, other jurisdictions. For example, staff may be "stranded" overseas for prolonged periods during work/personal travels because of changing rules on border controls and travel restrictions imposed by different governments to manage the pandemic.

Risks from lack of wet-ink signatures

- When an FI executes contracts using electronic/digital signatures in place of wet-ink signatures, there are potential risks in terms of recognition and enforceability of these contracts if the FI does not ensure compliance with the applicable laws and specific contractual requirements.

B. Key risks of remote working to FIs' operations

4. Legal and regulatory risks

Key risk management actions

FIs consider legal and regulatory implications when establishing guidance on remote working practices. These include practices on human resource management and the making of legal contracts, especially where transactions and activities involve foreign jurisdictions.

Examples of mitigating controls

Managing legal risks from FI's staff working remotely

- Remind supervisors to track and manage working hours of staff where necessary, particularly for jurisdictions with labour laws on staff's working hours.
- Implement policies and procedures to guide staff on appropriate remote working practices, including information security.
- Establish guidelines and protocols on staff working from other jurisdictions, including the obtaining of any prior approvals required by the laws of the other jurisdictions and the FI's internal policy. With the ongoing COVID-19 situation, staff travelling overseas risk being "stranded" for an indeterminable period if the rules on travel and border crossings change suddenly due to developments in the pandemic situation.

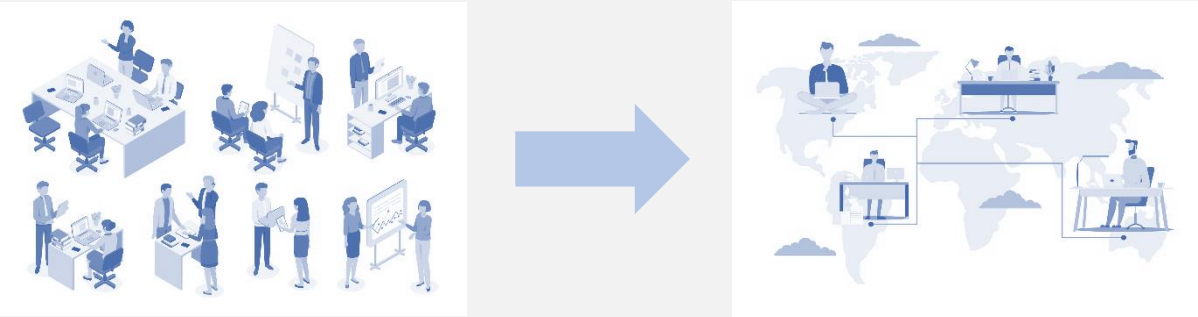
Managing legal risks from lack of wet-ink signatures

- Establish guidelines on the acceptance of electronic / digital signatures including, but not limited to:
  - the requirements of the Electronic Transactions Act in Singapore
  - factors to determine when case-by-case handling is required, and the appropriate escalation and approval procedures
- Where required, ensure proper indemnity and controls are in place before allowing the acceptance of electronic / digital signatures.
- Seek legal advice, if required, for contracts involving other jurisdictions.

C. Impact of remote working on people and culture

What has changed?

The sudden and large-scale shift of staff from working in the office to working remotely has changed the way people interact. Several FIs have started to implement hybrid working arrangements for the longer term.



Benefits of remote working

Surveys[2] show that the large majority of staff viewed the shift to remote working positively.

1. ***Staff work-life harmony*** - Despite reporting that they put in longer hours when working remotely, many staff do not wish to return to the office full-time even post-pandemic. To staff, remote working offers the flexibility to better achieve work-life harmony, and to use the significant time saved from their daily commutes more meaningfully (like for exercise). Staff who are better able to achieve work-life harmony are generally happier, leading to higher level of engagement.

2. ***Staff productivity*** – Contrary to employers' concerns that staff will be less productive without the presence of their managers, staff report being equally or more productive when working remotely. The reasons for this include reduced stress without the daily commute, and fewer interruptions from co-workers. Staff also report taking fewer days of sick leave for minor ailments – possibly because of less exposure to bacteria and viruses without the daily commute, and to other colleagues in the office who may be ill.

3. ***Talent recruitment and retention*** - The ability of organisations to offer staff a choice of flexible work arrangements could well be a key differentiating factor for attracting and retaining talented individuals, particularly individuals with in-demand skills for the new digital economy. With remote working, the talent pool available to organisations could potentially be expanded beyond individuals who are able and willing to relocate to be near the office.

[2] Routley, N.. 2020. How People and Companies Feel About Working Remotely. (https://www.visualcapitalist.com/how-people-and-companies-feel-about-working-remotely/), Frankiewicz
B. & Chamorro-Premuzic, T.. 2020. The Post-Pandemic Rules of Talent Management. (https://hbr.org/2020/10/the-post-pandemic-rules-of-talent-management)

C. Impact of remote working on people and culture

What are the risks?

The impact of remote working on an organisation's people and culture is not all positive, and has to be managed intentionally. Two broad areas to pay attention to are:

1. Staff welfare and well-being

Even as the majority of workers want the flexibility to work remotely post COVID-19, remote working may not be ideal for everyone - much depends on an individual's personal circumstances and temperament. Some staff do not have a conducive place at home to work effectively due to space constraints, or may face competing family demands. When staff are not given a choice in the matter of their work arrangements, remote working may cause significant emotional and mental stress for them.

2. Organisational culture and conduct

Even as there are many articles heralding the arrival of remote working as the new normal, there are other articles warning about the long-term adverse effects that remote working may have on an organisation's culture, team dynamics, creativity and overall ability to innovate.

Many organisations have found that the relationships among co-workers, formed prior to the mass exodus of workers from offices, have so far sustained ongoing collaborations in the virtual space. However, there are concerns that the lack of face-to-face interactions would, over time, erode existing bonds while reducing occasions to build new ties (particularly for new joiners), and thereby dilute team cohesion and shared norms.

Key risk management actions

FIs pay attention to staff's morale and welfare, and provide resources for their emotional and mental support. FIs also explore ways to build strong corporate culture and conduct in a remote or hybrid working environment.

C. Impact of remote working on people and culture

Examples of challenges and mitigating controls

1. Staff welfare and well-being

Common challenges

Unsuitable remote working environment

E.g. staff may be sharing small living space with a large family, or other tenants, all working from home or doing home-based learning at the same time, or be living near noisy construction sites or neighbours

Blurred lines between work and personal life

E.g. staff may be expected by family to attend to other matters for the home during work hours; staff may work longer hours without a commute to provide a distinct break between work and home, or because supervisors expect them to be available 24/7

Disengagement & unhappiness

E.g. staff working remotely may feel isolated from lack of face-to-face interactions, particularly if they live alone; other staff not allowed to work remotely because of their specific roles may be unhappy about perceived unfairness

Stress over performance

E.g. staff may be uncertain about appraisal criteria in remote working environment and feel pressured to compensate for loss of face-time with supervisors by working longer hours

C. Impact of remote working on people and culture

Examples of challenges and mitigating controls

1. Staff welfare and well-being

Examples of mitigating controls

Communication

- Increase communication by senior management, such as through virtual townhalls, to keep staff connected
- Explain decisions in a clear and transparent manner to get buy-in, such as reasons for why particular functions or roles cannot be performed remotely
- Implement feedback avenues (e.g. regular sentiment surveys, confidential feedback / whistleblowing channels) for staff to raise concerns safely, so that management can understand and address them.

Additional resources

- Provide resources for help, such as curated articles and webinars on maintaining mental well-being and stress management, and free and confidential professional counselling sessions
- Provide additional benefits, such as monetary allowance to offset costs of remote working, or the provisioning of IT equipment for staff to work from home

Emotional & mental support

- Increase check-ins by supervisors on individual staff members to monitor signs of fatigue, stress and emotional distress, and if they are taking vacation leave to rest and recharge
- Show empathy and sensitivity towards staff members' unique personal circumstances
- Provide social support through a buddy system or virtual informal / recreational activities

Performance appraisal

- Train supervisors to assess staff's performance by outcomes and not mere presenteeism
- Communicate performance goals clearly
- In appraisal discussions, demonstrate equity and fairness in work allocation and performance reviews

C. Impact of remote working on people and culture

Examples of challenges and mitigating controls

2. Organisational culture and conduct

Common challenges[3]

Harder for management and supervisors to remotely ***role model desired ethical behaviour, corporate values and code of conduct*** – risk of dilution of organisation's culture

Harder to ***maintain close bonds*** virtually; more difficult to sustain team camaraderie – risk of staff losing sense of belonging and loyalty to organisation

Harder to ***integrate new joiners*** into the organisation if they do not spend sufficient time with team members – risk of new joiners feeling disengaged from the organisation

Less opportunities for ***spontaneous collaboration*** across teams, if teams work in silos – risk of impeding culture of creativity and innovation in the organisation

[3] Parke, M.. 2020. If Pandemic Productivity Is Up, Why Is Innovation Slowing Down? (https://knowledge.wharton.upenn.edu/article/pandemic-productivity-is-up-why-is-innovation-slowing-down/).

C. Impact of remote working on people and culture

Examples of challenges and mitigating controls

2. Organisational culture and conduct

Despite the challenges in nurturing an organisation's culture in a remote working environment, Gallup[4] suggests that the *"new normal is an opportunity to redefine the behaviours and rituals that codify the cultural values leadership wants to be reflected across the employee experience."* Its studies indicate that organisations which align the virtual, hybrid and in-person staff experience of workplace culture, by consistently upholding core values in communications and decisions made, are most effective in creating a shared culture.

Examples of mitigating controls[5]

[4] Hickman, A. & Morgan, I.. 2020. Redefine (Don't Redesign) Your Culture for the Virtual Workplace. (https://www.gallup.com/workplace/322307/redefine-don-redesign-culture-virtual-workplace.aspx)

[5] Based on ABS ROOT member inputs.

D. Illustrations

This section provides examples of key remote working risks of specific functions.

Illustration 1: Fraud risks in anti-money laundering and countering the financing of terrorism

Changes: FIs have adjusted **Know-Your-Customer (KYC)** verification processes to facilitate remote working during the pandemic.

Before remote working ("In-person KYC")	After remote working ("Remote KYC")
• Meet customer face-to-face for onboarding and periodically over course of relationship	• Conduct meetings virtually over audio and/or video calls
• Verify identity of customer[6] by physically sighting original identification and other required documents	• Verify identity of customer[6] by relying on copies and requesting customer to show original identification documents over video calls
• Physically observe customer signing application forms and other agreements, or require customer's wet-ink signature before acting on instructions, such as to open accounts and transfer funds	• Accept electronic/digital signatures for application forms/other agreements and instructions over calls / emails if appropriate indemnities are in place

Risks: "Remote KYC" controls are more susceptible to fraud risks, such as identity theft and forgery of documents / signatures, than "in-person KYC" controls.

Mitigating controls: Based on risks of money-laundering and terrorism financing posed by a customer, supplement "remote KYC" controls with "in-person KYC" controls.

[6] Including beneficial owners, directors and authorised signatories

D. Illustrations

Illustration 2: Staff misconduct risks in trading function

The trading activity is one of the most tightly controlled functions in an FI. This is partly because of the potential significant financial impact from any single trade and the speed at which trades occur. This is also partly because of the relatively higher inherent risk of staff misconduct due to the risk-taking nature of the business.

Following several high-profile incidents of misconduct by errant dealers over the years, dealers are subjected to strict risk and compliance controls when working in the office. The modification and relaxation of these controls, required to allow dealers to trade remotely, expose FIs to higher inherent risk of dealer misconduct.

Consequently, FIs are generally reluctant to allow traders to work remotely. However, if circumstances (like the pandemic) require, FIs should ensure remote working risks are adequately mitigated.

WIO controls

- Trading activity conducted in enclosed dealing room with access restricted to authorised personnel; trading systems accessible only from dealing room; after-hours trading tightly controlled.
- Dealers' conversations on all communication mediums are recorded and monitored. Use of personal mobile phones and devices prohibited.
- Dealers' activities closely watched by dedicated compliance and risk management teams within the dealing room and via risk management systems.

Changes with remote working

- Trading activities potentially conducted anywhere and anytime.
- Dealers' conversations held over softphones, mobile apps or dealing systems with recording functions, as far as possible.
- Dealers' activities monitored remotely by dedicated compliance and risk management teams.

Risk management challenges

- FIs unable to ascertain if unauthorised parties are listening in to dealers' conversations leading to information leakage.
- FIs without recording capabilities rely on email confirmations to / from counterparties, or rely on team of WIO dealers to record trades – unable to check dealers' actual conversations.
- Errant dealers may be emboldened to collude and commit fraud with the reduced oversight

D. Illustrations

Illustration 2: Staff misconduct risks in trading function

Examples of controls to mitigate the risks of dealers trading remotely[7]:

- Establish policies and guidelines on permitted locations where trading can be performed remotely, and to require dealers to confirm remote working locations daily or report/seek approval for deviations.
- Enhance surveillance of dealers' remote working activities, such as by:
  - Increasing the monitoring of dealers' conversations on recorded channels
  - Expanding the sampling of booked trades to ensure they were transacted over permitted channels, and "cancel and amend" trades to ensure that they are valid
  - Using data analytics and technology to detect anomalies like unusual trading patterns and key strokes used

[7] Based on ABS ROOT member inputs and Spezzati, S.. 2020. With Traders Far From Offices, Banks Bring Surveillance to Homes. (https://www.bloomberg.com/news/articles/2020-10-16/with-traders-far-from-offices-banks-bring-surveillance-to-homes)

In conclusion…

The financial sector has adapted well to the rapid and large-scale shift to remote working necessitated by the COVID-19 pandemic. The pandemic situation continues to evolve, with countries experiencing resurgences of cases and the emergence of new variants of the virus. FIs should remain vigilant and be alert to developments and any new remote working risks that may emerge over time.

As FIs consider the adoption of various hybrid working arrangements in the new normal, they should abide by fundamental risk management principles while exploring new forms of controls to manage risks.

Given the importance of the financial sector to the Singapore economy, it is vital that FIs ensure that risk management remains a priority even with remote working. Lapses and losses not only affect FIs and customers, but also the public's perception of, and trust in, Singapore's financial sector.

MAS and ABS will continue to work together to understand emerging remote working trends and any corresponding risks, and identify best practices to maintain high standards of risk management for Singapore's financial sector.

Acknowledgements

A. The paper is published jointly by the Monetary Authority of Singapore and The Association of Banks in Singapore (ABS) Return to Onsite Operations Taskforce (ROOT).

ABS ROOT is formed to provide members with a platform to share and coordinate responses to the COVID-19 situation and plan for the post-COVID "new normal". ABS ROOT also consolidates good practices by its members, and shares them by (i) conducting industry briefings for ABS member banks/institutions and other industry associations, and (ii) addressing queries from the briefings' participants. ABS ROOT, which is supported by eight Workstreams, has been deeply involved in assessing the operational changes and challenges triggered by COVID-19. ABS ROOT has expanded its coverage beyond focusing on onsite and retail activities to reviewing forward-looking human resource practices, future workspaces, new remote working risks, sustainability practices, and also finding ways for technology to play an active role in the delivery of solutions.

Workstream 8, which focuses on remote working risks, has collaborated with MAS to co-publish this information paper. Members from ABS ROOT Workstream 8 are:

- Bank of America NA, Singapore Branch
- Bank of China Limited, Singapore Branch
- Barclays Bank PLC, Singapore Branch
- Citibank Singapore Limited
- DBS Bank Limited
- Deutsche Bank AG Singapore Branch
- HSBC Bank (Singapore) Limited
- Maybank Singapore Limited
- Network for Electronic Transfers (Singapore) Pte Ltd
- Oversea-Chinese Banking Corporation Limited
- Standard Chartered Bank (Singapore) Limited
- United Overseas Bank Limited

B. Graphics from Dreamstime.com