Issue 01/2021
www.bdo.com.sg

Newsletter

Regulatory Updates for Fund Management Companies

Welcome to the first quarterly newsletter of the BDO Regulatory Updates for Fund Management Companies for the Year 2021. This newsletter serves as a summary of the key regulatory developments for fund management companies or capital markets services licensees covering the period from January 2021 to March 2021.

CONTENTS

REGULATORY DEVELOPMENTS

From January 2021 to March 2021, the MAS has issued or updated a series of Guidelines, Circulars and Information Papers as well as published some Enforcement Actions including a joint investigation by the regulators for possible offences under the Penal Code and the Securities and Futures Act.

Guidelines on Risk Management Practices – Technology Risk

Status	First Issue date: **21 June 2013** Revision date: **18 January 2021** Effective date: **18 January 2021**

- The Monetary Authority of Singapore ("MAS") has issued the revised Technology Risk Management Guidelines ("TRM Guidelines").
- The TRM Guidelines were developed primarily to keep pace with the fast-changing cyber threat landscape as well as emerging technologies with increased reliance by the financial institutions ("FIs") on cloud technologies, application programming interfaces ("APIs") and rapid software development as well as the increased data sharing by FIs.
- The TRM Guidelines aim to support FIs by providing a framework of best practices in overseeing technology risk governance, practices, and controls to address technology and cyber risks.
- FIs should carefully review the TRM Guidelines and make adjustments based on the size, nature and complexity of their businesses. The Guidelines provide general guidance that expounds on the mandatory requirements set out in the MAS Notice on Technology Risk Management, without intending to replace or override any legislative provisions. They reflect the MAS' expectations for TRM and security controls within the FIs, but are not to be regarded as a statement of the standard of care owed by the FIs to their clients.

- Below are the key amendments made in the current TRM Guidelines:

1. ***Additional guidance on the expanded roles and responsibilities of the Board of Directors and Senior Management***

MAS has clarified that the intent of the following changes, is for the FI's Board and Senior Management to comprise members who are able to competently exercise their oversight of the FI's technology strategy, operations and risks.

The 2013 TRM Guidelines:	The Current TRM Guidelines:
▪ The Board and Senior Management have general oversight of the technology risks of the FIs.	▪ The Board and Senior Management should ensure that a Chief Information Officer (or its equivalent), with the requisite experience and expertise, are appointed to accountable for managing technology and cyber risks.
▪ The Board and Senior Management are involved in key IT decisions.	▪ The Board and Senior Management should include members with knowledge of technology and cyber risks.
▪ The Board and Senior Management are required to: - ensure that a sound and robust technology risk management framework, is established and maintained - be fully responsible for ensuring that effective internal controls and risk management practices, are implemented to achieve security, reliability, resiliency, and recoverability - give due consideration to cost-benefit issues, including factors such as reputation, customer confidence, consequential impact and legal implications, with regard to investment in controls and security measures for computer systems, networks, data centers, operations and backup facilities.	▪ The Board and Senior Management's responsibilities for technology risk management is extended as follows: a. **the Board is responsible for:** - ensuring a sound and robust risk management framework is established and maintained to manage technology risks; - ensuring a technology risk management function to oversee the TRM framework and strategy, as well as to provide an independent view of the technology risks that faced by the FI; - giving senior executives, who are responsible for executing the FI's TRM strategy, sufficient authority, resources and direct access to the Board of Directors; - approving the risk appetite and risk tolerance statement that articulates the nature and extent of technology risks that the FI is willing and able to assume; - assessing management competencies for managing technology risks; and - ensuring an independent audit function is established to assess the effectiveness of controls, risk management and governance of the FI. b. **Senior Management is responsible for:** - establishing the TRM framework and strategy; - managing technology risks based on the established framework and strategy; - ensuring sound and prudent policies, standards and procedures for managing technology risks are established and maintained, and that standards and procedures are implemented effectively; - ensuring the roles and responsibilities of staff in managing technology risks are delineated clearly; and - apprising the Board of Directors of salient and adverse technology risk developments and incidents that are likely to have a major impact on the FI in a timely manner.

2. ***New guidance on the management of information assets***

The 2013 TRM Guidelines:	The Current TRM Guidelines:
▪ No specific provisions about information asset management practices.	▪ Introduce a requirement to establish information asset management practices that include the following: - identification of information assets that support the FI's business and delivery of financial services; - classification of an information asset based on its security classification or criticality; - ownership of information assets, and the roles and responsibilities of the staff managing the information assets; and - establishment of policies, standards and procedures to manage information assets according to their security classification or criticality. - Expect FIs to maintain an inventory of all its information assets. - Review and update the inventory periodically whenever there are changes.

3. ***More stringent assessments of third-party vendors and entities that access the FI's IT systems***

a. **Assessment of Vendors**

The 2013 TRM Guidelines:	The Current TRM Guidelines:
▪ Need FIs to be careful in their selection of the vendors and contractors and to implement a screening process when engaging them.	▪ Introduce a requirement for the FI to establish standards and procedures for vendor evaluation that is commensurate with the criticality of the project deliverables to the FI. ▪ Expect FIs to conduct assessment of the service providers' exposure to various technology risks associated with the loss of data confidentiality, integrity and service availability, thereafter, manage the associated risks, as well as appropriate due diligence. ▪ Specify that the assessment to include, amongst others, a detailed analysis of the vendor's software development, quality assurance and security practices in place to safeguard and protect any sensitive data accessible over the course of services.

The MAS has clarified that FIs may adopt a risk-based approach when assessing the robustness of their software vendor's security and quality assurance practices.

FIs may also obtain an undertaking from the software vendor on the quality of the software to gain assurance that, the third party's software is secure.

b. **Assessment of third parties' suitability in connecting to the Application Programming Interface ("APIs") and governing third party's API access**

The 2013 TRM Guidelines:	The Current TRM Guidelines:
▪ No specific provisions governing API access.	▪ Introduce an entirely new requirement for FIs to develop a well-defined vetting process for the assessing third party entities who wish to access their API and for governing the nature of the API access. - The vetting process includes, amongst others, evaluating the third party's nature of business, cyber security posture, industry reputation and track record. ▪ Expect FIs to consider a list of additional requirements as per the TRM Guidelines.

With regards to the scope of the guidelines on APIs, the MAS has indicated that the key aspects are to:

i. use strong encryption to securely transmit sensitive data;

ii. build capabilities to monitor the usage of APIs; and

iii. detect suspicious activities and revoke any access in the event of a security breach.

For references of best practices, the MAS recommends the MAS-ABS Financial World: API Conference 2016 E-book and the ABS-MAS Financial World: Finance-as-a-Service API Playbook.

4. ***Introduction of monitoring, testing, reporting and sharing of cyber threats within the financial ecosystem***

a. **Cyber Threat Intelligence and Information Sharing:**

The 2013 TRM Guidelines:	The Current TRM Guidelines:
▪ No specific provisions governing cyber related information. ▪ Provided general suggestions for FIs to implement security solutions to adequately address and contain threats to their IT environments.	▪ Introduce the guidance that FIs should establish a process of collecting, processing and analysing cyber related information. ▪ Expect FIs to procure cyber intelligence monitoring services. FI should actively participate in cyber threat information-sharing arrangements with trusted parties to share and receive timely and actionable cyber threat information. ▪ Expect FIs to establish a process to detect and respond to the misinformation related to the FI that are propagated via the internet. FIs should consider engaging external media monitoring services to facilitate the evaluation and identification of online misinformation. ▪ Provide that FIs should establish a security operations center or acquire managed security services in order to facilitate the continuous monitoring and analysis of cyber events.

The MAS has however clarified that it does not require FIs to subscribe to any specific cyber threat intelligence monitoring and sharing services. The intent is for the FI to participate in cyber threat information sharing arrangements with trusted parties where appropriate.

b. Cyber Incident Response and Management:

The 2013 TRM Guidelines:	The Current TRM Guidelines:
▪ Provided for a general incident management plan for a disruption to the standard delivery of information technology services.	▪ Provide that the FIs should establish a cyber incident response and management plan to swiftly isolate and neutralise a cyber threat and to securely resume any affected services. This introduces a need to FIs to establish a process to investigate and identify the security or control deficiencies and lay out the communication, coordination and response procedures to address plausible cyber threat scenarios.

c. Cyber Security Assessments – Vulnerability Assessment and Penetration Testing:

The 2013 TRM Guidelines:	The Current TRM Guidelines:
Provided for: ▪ a general guidance on regular vulnerability assessment to detect security vulnerabilities in the IT environment. ▪ FIs to deploy a combination of automated tools and manual techniques to perform a comprehensive vulnerabilities assessment. ▪ FIs to establish a process to remedy issues identified in the vulnerability assessments and perform subsequent validation of the remediation to validate that, all gaps are fully addressed.	▪ Provide that the FIs should assess their cyber security through vulnerability assessment and penetration testing. ▪ Dictate that the minimal requirements of the vulnerability assessment, should include the vulnerability discovery process, an identification of weak security configurations and open network ports as well as the penetration testing to evaluate its cyber security defences. ▪ Require FIs to perform a combination of blackbox and greybox testing for online financial services during the penetration testing. This represents a marked expansion of the original scope of vulnerability assessment and penetration testing as laid out in the 2013 Guidelines.

The MAS has indicated that the risk assessment of an FI's environment, especially the cyber security assessment, should form an integral part of the FI's efforts in mitigating security threats and systems' vulnerabilities.

d. Cyber Exercises - Simulation of Cyber-attacks, Techniques and Procedures:

The 2013 TRM Guidelines:	The Current TRM Guidelines:
▪ Provided a general comment that simulations of actual attacks could be carried out as part of a penetration test.	▪ Provide that the FIs should carry out regular scenario-based cyber exercises to validate their response and recovery plan. These exercises should involve the Senior Management, business functions, technical staff responsible for cyber threat detection, response and recovery and other relevant stakeholders. ▪ Specify that the exercises should be in the form of an adversarial attack by a red team in order to test and validate the effectiveness of its cyber defence and response plan. ▪ Expect that a comprehensive remediation process should follow after the exercise.

The MAS has clarified that the intent of these simulations is to obtain an accurate evaluation of the robustness of the FI's cyber defences to ensure adequate protection.

Circular on the Developments in Myanmar

Status	First Issue date: **25 February 2021** Effective date: **25 February 2021**

- In response to the media queries dated 23 February 2021, the MAS mentioned that its regular surveillance of the banking system has not found significant funds from Myanmar companies and individuals in banks in Singapore.
- The MAS reminds financial institutions in Singapore of the following:
  - to keep abreast of the fast-developing situation in Myanmar, including unilateral sanctions imposed by other jurisdictions;
  - to take appropriate measures to manage any risks arising from the business activities and customer relationships, including reputational, legal and operational risks;
  - to comply with MAS regulations that implement United Nations Security Council resolutions, continue to monitor all transactions and fund flows, and stay vigilant to any suspicious transaction or fund flow between Singapore and Myanmar;
  - to apply enhanced customer due diligence and appropriate risk mitigation measures in higher-risk situations; and
  - to file a suspicious transaction report (STR) when suspicion aroused, by indicating "Myanmar 2021" upfront in the "Reasons for Suspicion" field.
- MAS closely supervises financial institutions to check that processes are in place for compliance and takes appropriate enforcement actions where there are serious lapses.

Information Paper on Risk Management and Operational Resilience in Remote Working Environment

Status	First Issue date: **3 March 2021** Effective date: **3 March 2021**

- The MAS and The Association of Banks ("ABS") in Singapore have jointly issued a paper on managing new risks that could emerge from extensive remote working arrangements adopted by financial institutions ("FIs") amid the COVID-19 pandemic.
- 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"), includes reputational risk, credit risk and market risk.
- The paper has highlighted the possible key risks of remote working to FIs' operations and key actions that FIs are encouraged to adopt, to manage the remote working risks, as follows:

1. **Operational Risks**	
a. **Changes in Control Environment** i. Policies and procedures originally implemented for an office-setting, have been adapted or amended to facilitate remote working. ii. 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. iii. Certain systems and confidential information that were previously accessible only from the office are now accessible remotely. iv. Assessments that used to rely on physical meetings and site visits are now done through virtual meetings. v. Verifications that were previously performed against original documents are now conducted based on softcopies.	
Risks	▶ Inadequately assessing risk implications of allowing specific functions to be performed remotely on a large-scale and over a prolonged period, leading to inadequate steps taken to: - manage these risks; - keep them within the FIs' overall risk appetite limits; or - seek approval from the boards and senior management for deviation from these limits.

Key Risk Management Actions	i. FIs to review remote working arrangements to identify risks from changes in control environment and processes. ii. FIs to implement compensating controls to manage identified risks within risk appetite statements approved by Board and senior management. iii. FIs to adopt robust change management procedures so that staff understand and implement the new processes and controls as intended.
Examples of Mitigating Controls – Short Term Measures	i. FIs' BSM review and approve risk appetite statements / limits for remote working. ii. 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). iii. 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). iv. 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). v. 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).
Examples of Mitigating Controls – Medium to Longer Measures	i. 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. ii. 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. iii. Digitise hardcopy documents where possible and digitalise workflows and processes, including implementing more system controls, to reduce reliance on manual processes. iv. Conduct ongoing assessment of remote working risks and effectiveness of mitigating controls, such as through control self-assessments and internal audits, etc.
b. **Outsourcing and Other Third-Party Arrangements** ▶ Adopting remote working by FIs' vendors may change the way services are delivered under these arrangements, and potentially vendors' risk profiles. The staff of both FIs and vendors work remotely, leading to the possibility of FIs facing challenges in conducting physical audits and site visits.	
Risks	i. 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. ii. For vendor services that 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. iii. 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	i. FIs to evaluate changes to vendors' risk profiles with remote working, such as by assessing vendors' remote working controls and operational resiliency. ii. FIs to implement appropriate safeguards and contingency plans to ensure continuity of services.

Examples of Mitigating Controls – Short Term Measures	i. 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. ii. Increase monitoring of vendors' performance for timely identification of issues, such as delays or lapses in service delivery standards. iii. Increase communications with vendors to understand and resolve performance issues in timely manner.
Examples of Mitigating Controls – Medium to Longer Term Measures	i. 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. ii. 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. iii. 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.
c. **Business Continuity Management Risk** ▶ 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.	
Risks	▶ With large-scale remote working, effects of disruptions in remote working situations may be compounded if the recovery team members: i. are unable to obtain prompt technical support for their hardware issues, which is typically readily available when WIO. ii. remote working locations are not supported by uninterruptible power supply and/or back-up generators in the event of power outages. iii. have no alternative means to connect to the office network when working remotely if there are disruptions in internet or VPN services.
Key Risk Management Actions	▶ FIs to 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	i. Enhance scope of business continuity plans to cover disruptions in remote working situations and include them in scenario testing. ii. Make arrangements for staff to resolve hardware issues and access an alternative work location if required. iii. 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.
2. **Information Security and Technology Risks**	
a. **Information Governance** ▶ 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.	

Risks	▶ Allowing staff to access customer and other sensitive information remotely heightens inherent risks of leakage, such as through: i. Shoulder surfing and eavesdropping by family members or strangers. ii. 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. iii. 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). iv. Staff surfing the internet via the internet service provider (ISP) directly on corporate devices bypassing corporate proxy / internet gateway.
Key Risk Management Actions	i. FIs to assess the risks and implications of information loss when determining which activities can be performed remotely. ii. FIs to strengthen preventive and detective controls to mitigate these risks.
Examples of Mitigating Controls – Preventive Measures	i. 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). ii. Establish policies, standards and procedures on handling sensitive information remotely. iii. Remind staff to safeguard sensitive information. iv. Grant remote access to information only on a need-to basis. v. Disable USB ports and Bluetooth to prevent printing and transfer of information. vi. Disallow storage of corporate data on personal device, if device not managed by corporate policies. vii. Implement Data Loss Protection monitoring tools to prevent and detect data leakage. viii. Disable VPN split tunneling and/or enable always-on VPN configuration.
Examples of Mitigating Controls – Detective Measures	i. 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). ii. Increase call monitoring and other staff surveillance activities for high-risk functions (e.g. trading, investment advisory). iii. 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. **Cybersecurity** ▶ 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.	
Risks	i. A cyber-attack targeting an FI's remote access infrastructure could potentially disrupt its availability and affect remote users. ii. Internet set-up in a staff's home or chosen remote working location is generally more difficult to secure than an office-based network. iii. 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 to implement controls to ensure that staff's remote working infrastructure, including personal devices, are secured.

Examples of Mitigating Controls	i. Implement redundancies and reduce single points of failure in remote access infrastructure. ii. Increase staff's vigilance of phishing and social engineering scams through regular security awareness programs. iii. Implement multi-factor authentication for remote access. iv. Ensure that remote access infrastructure is appropriately configured and secured. v. Assess and address risks from use of personal devices to access corporate resources remotely. vi. 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. vii. Perform penetration testing on remote access infrastructure. viii. Provide staff with securely configured mobile router for internet connection if necessary. ix. 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).
c. **Information Technology Assets Management** ▶ 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.	
Risks	i. 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. ii. 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	i. Maintain updated inventory list of all hardware and software assets. ii. 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. iii. Remind staff to safeguard IT assets issued to them. iv. Ensure that corporate-issued devices used for remote working conform to FIs' security standards and implement hard disk encryption. v. Implement and test disaster recovery plans of the newly implemented hardware and software
3. **Fraud and Staff Misconduct Risks**	
a. **Fraud** ▶ Remote working has required changes to certain business practices. For example: i. virtual meetings and calls have replaced face-to-face meetings with customers and site visits. ii. soft copies of documents are now accepted in place of original documents. iii. digital signatures are used instead of wet-ink signatures. iv. 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.	

Risks	i. 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). ii. 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 iii. 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	i. FIs keep abreast of evolving fraud typologies from remote working and implement appropriate preventive and detective controls. ii. FIs implement guidelines to identify situations where in-person meetings, site visits and verification against original documents are required.
Examples of Mitigating Controls – Create Customer Awareness	i. Run fraud risk awareness campaigns for customers (e.g. on digital banking platforms, social media, webinars). ii. Promote use of digital banking channels for transactions as an alternative to call instructions. iii. Encourage use of trusted official sources (e.g. MyInfo) to authenticate identity for onboarding, where possible.
Examples of Mitigating Controls – Maintain Staff Vigilance	i. Conduct fraud risk training for staff with tailored guidance for specific functions (e.g. phishing simulation exercises). ii. Remind staff to be vigilant for fraud. iii. Establish internal escalation procedures to handle suspicious activities and transactions.
Examples of Mitigating Controls – Preventive Measures	i. 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). ii. 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. iii. 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. iv. 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. v. 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.
Examples of Mitigating Controls – 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. **Staff Misconduct** ▶ With remote working, staff no longer work under the physical oversight of supervisors or in the physical presence of colleagues.	
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: i. Staff circumventing work processes and controls (e.g. transmitting confidential information over unauthorised channels to avoid FI's surveillance applications). ii. 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. iii. Staff communicating inappropriately with customers/counterparties (e.g. making misleading statements, especially on unrecorded devices).
Key Risk Management Actions	i. FIs adopt and communicate appropriate incentive structures and consequence management frameworks to drive the right behaviour even when staff are working remotely. ii. FIs enhance the monitoring of activities and transactions of staff in high-risk roles.
Examples of Mitigating Controls – Preventive Measures	i. Remind staff to comply with the FI's Code of Conduct, policies and procedures. ii. Encourage supervisors to regularly engage staff (e.g. through daily team calls). iii. Share lessons learnt from operational lapses and misconduct incidents as reminders. iv. 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).
Examples of Mitigating Controls – Detective Measures	i. 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. ii. 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).
4. **Legal and Regulatory Risks**	
i. The extent of the adoption of remote working by FIs has materially increased due to the pandemic. ii. To facilitate remote working, FIs have accepted certain modes of electronic/digital signing of documents, in place of wet-ink signatures.	
Risks from FIs' staff working remotely:	i. 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. ii. 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. iii. 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. iv. 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). v. 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.
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	i. Remind supervisors to track and manage working hours of staff where necessary, particularly for jurisdictions with labour laws on staff's working hours. ii. Implement policies and procedures to guide staff on appropriate remote working practices, including information security. iii. 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.
Examples of Mitigating Controls – Managing legal risks from Managing legal risks from lack of wet-ink signatures	i. 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 ii. Where required, ensure proper indemnity and controls are in place before allowing the acceptance of electronic / digital signatures. iii. Seek legal advice, if required, for contracts involving other jurisdictions.

- On the impact on people and culture that may be brought about by remote working, FIs should pay attention to staff's morale and welfare, and provide resources for their emotional and mental support. FIs should also explore ways to build strong corporate culture and conduct in a remote or hybrid working environment.
- The Paper suggests key risk management actions and examples of mitigating controls drawn mainly from the experiences of ABS' Return to Onsite Operations Taskforce member banks. Despite so, many of the risks and mitigating controls set out in the paper are also relevant and applicable to non-bank FIs. Hence, MAS strongly encourages all FIs to assess the remote working risks and benchmark the corresponding controls against the examples.

February 2021 FATF Statement

Status	First Issue date: **6 March 2021** Effective date: **6 March 2021**

1. The MAS has published the FATF Statement for February 2021, that the FATF has continued to pause the review process for the list of "High-Risk Jurisdictions subject to a Call for Action".
2. Hence, the MAS advises the FIs to continue to refer to the previous FATF Statement issued in February 2020, which highlights the strategic deficiencies in the anti-money laundering or combating the financing of terrorism ("AML/CFT") regimes of the Democratic People's Republic of Korea ("DPRK") and Iran.
3. While the statement may not necessarily reflect the most recent status in DPRK and Iran, due to the pause in the review process, the FATF's call for action on these high-risk jurisdictions remains in effect.

▶ On DRPK:
The FATF remains concerned by its failure to address the significant deficiencies in its AML/CFT regime and the serious threats they pose to the integrity of the international financial system.
The FATF urges the DPRK to immediately and meaningfully address its AML/CFT deficiencies. The FATF has serious concerns with the money laundering, terrorism financing and proliferation financing risks posed by DPRK's illicit activities.
DPRK is subject to the FATF's call on countries to apply counter-measures and FIs should give special attention to business relationships and transactions with links, whether directly or indirectly, to the DPRK.
Countries and FIs are called to apply effective counter measures, targeted financial sanctions, and other measures in accordance with the applicable United Nations Security Council Resolutions ("UNSCRs").

▶ On Iran:
Since Iran's action plan has expired in January 2018 and in February 2020 respectively, the FATF has noted that Iran has not completed its action plan.
Given Iran's continued failure to enact the Palermo and Terrorist Financing Conventions to be in line with the FATF Standards, the FATF has decided in February 2020 to fully lift the suspension of counter-measures.
FATF members and FIs are called to apply effective counter-measures, in line with Recommendation 19. The FATF remains concerned with the terrorism financing risk emanating from Iran and the threat this poses to the international financial system.

- In considering the range of counter-measures, FIs in Singapore should consider both DPRK and Iran as high risk jurisdictions and apply enhanced due diligence measures accordingly.

Publication of Enforcement Actions on Breaches or Investigations on Potential Breaches of Regulatory Requirements

Status		
	First Issue date:	**1 February 2021**
	Second Issue date:	**3 March 2021**
	Third Issue date:	**15 March 2021**
	Fourth Issue date:	**15 March 2021**

1. The Singapore Police Force and the MAS investigate companies under CoAssets Group:

- The Commercial Affairs Department ("CAD") of the Singapore Police Force and the MAS have launched a joint investigation into various companies under CoAssets Ltd (CoAssets Group Companies) for possible offences under the Penal Code (Cap. 224) and the Securities and Futures Act (Cap. 289, "SFA"). The joint investigation stems from complaints and feedback received from members of the public regarding suspected misconduct by CoAssets Group Companies.
- Of the CoAssets Group Companies, only CA Funding Pte Ltd ("CAFPL") is regulated by MAS, as a capital markets services licensee. In March 2020, MAS has issued a direction to CAFPL to prohibit the company from listing new issuances, onboarding new investors and accepting subscription of securities. These directions were issued after MAS' inspection uncovered lapses in CAFPL's credit assessment process, inadequate disclosure of information to investors, and failure to address conflicts of interests arising from dealings that the CoAssets Group Companies had with entities related to issuers that CAFPL had listed on its platform. MAS also directed CAFPL to appoint an independent external auditor to review the effectiveness of its remedial measures to address these deficiencies.
- CAFPL informed the MAS in December 2020 that it had failed to comply with the minimum base capital requirement under the SFA and intended to cease operations. Pursuant to directions issued to CAFPL by MAS, all customers' moneys held by CAFPL have since been returned to investors. The MAS is closely monitoring CAFPL's implementation of its cessation plan, to ensure that investors are treated fairly.

2. **The MAS bans four individuals for market misconduct:**

- The MAS has issued prohibition orders ("POs") against the following four individuals, following their convictions for market misconduct offences:

Names	Former Positions	Duration of Prohibition Orders
Ms Lau Wang Heng	Former remisier of CGS-CIMB Securities (Singapore) Pte Ltd	10 years
Mr Yeo An Lun	Former representative of Prudential Assurance Company Singapore (Pte) Limited	6 years
Mr Goh Qi Run Rayson	Former remisier of OCBC Securities Private Limited	5 years
Mr Teo Boon Cheng	Former remisier of KGI Securities (Singapore) Pte Ltd	4 years

- These four individuals were among the eight individuals charged for offences under the SFA in relation to a scheme to commit false trading in the shares of Catalist-listed Koyo International Limited. They were convicted and sentenced to imprisonment terms of between 3 months and 20 months 18 weeks. They are also prohibited from providing any financial advisory services, or taking part in the management, acting as a director, or becoming a substantial shareholder of any licensed financial adviser under the Financial Adviser ("FAA"). In addition, Ms Lau, Mr Goh and Mr Teo are prohibited from carrying out any regulated activities and from taking part in the management, acting as a director, or becoming a substantial shareholder of any capital market services licensee under the SFA. The prohibition took effect from 1 March 2021.
- The MAS does not tolerate such misconduct and will take firm action to keep such offenders out of the financial industry. FIs are reminded not to employ or deal with any person who has been issued with a prohibition order by the Authority.

3. **The court convicted individual for false trading and deception:**

- Mr Wong Leon Keat was sentenced on 12 March 2021 to a total eight weeks' imprisonment and a fine of S$30,000 for false trading and deceiving a brokerage firm while trading in the shares of Gaylin Holdings Limited ("Gaylin"). His conviction was the result of a joint investigation conducted by the MAS and the referral by the Singapore Exchange Securities Trading Limited ("SGX-ST") to the MAS, for the following offences:
  - 17 charges under Section 197(1)(b) of the SFA, for creating misleading appearances with respect to the price of Gaylin shares on 17 occasions between 11 November 2015 and 25 October 2016;
  - A charge under Section 201(b) of the SFA, for deceiving UOB Kay Hian Private Limited by not disclosing his 50% beneficial interest in Gaylin shares bought using a UOB Kay Hian's trading account belonging to another individual; and
  - A charge under Section 182 of the Penal Code, for furnishing false information to the public officer investigating the case.
- The MAS emphasizes that it will take firm action against persons who engage in the misconduct of false trading and unauthorised trading, as these would undermine public confidence in the capital markets of the country.

4. **Envy Asset Management and Envy Global Trading are not licensed by the MAS:**

- With reference to the charges of cheating and fraudulent trading brought in the State Courts against Ng Yu Zhi, a director of Envy Asset Management Pte Ltd ("EAM") and Envy Global Trading Pte Ltd ("EGT"), the MAS announced that both EAM and EGT are not licensed by the Authority.
- EAM and EGT are believed to have been engaged in an investment fraud scheme between October 2017 and February 2021 involving the purported trading of nickel. Firms that deal in or invest funds for qualified investors in physical assets (i.e. not capital markets products), are not required to be licensed by MAS. This approach is broadly similar to that taken in other major financial centres. MAS is nevertheless examining EAM's and EGT's investment documents and other available evidence to see if they have been engaging in capital markets products or in any activity that would have required the two firms to obtain a MAS licence.

- On 19 March 2020, the MAS had placed EAM on the Investor Alert List, to highlight that EAM may have been wrongly perceived as being licensed by MAS. MAS had received public feedback that EAM had told customers that it was in the process of applying for a licence from MAS, when in fact no such application had been submitted. The MAS had subsequently received further information on transactions carried out by EAM, as well as its related entity, EGT. MAS had conducted a deeper review and shared its findings with the Commercial Affairs Department ("CAD").
- Mr Ng is alleged to have cheated Envysion Wealth Management Pte Ltd ("EWMPL"), a MAS-licensed fund manager and its founder and CEO, Shim Wai Han, of at least S$48 million. Following the CAD's commencement of investigations into EGT in February 2021, MAS has issued directions to EWMPL to:
  - cease accepting new monies for investment into EGT's nickel scheme;
  - inform affected investors of the Police investigation into EGT and the fund's status; and
  - appoint an independent third party to oversee all transactions of the fund's bank accounts.
- MAS is closely monitoring EWMPL's implementation of the directions, to ensure that investors are treated fairly. The MAS is also conducting a supervisory review of EWMPL to ascertain if there have been governance or risk management failures by its board and senior management. The MAS expects the licensed fund managers to practise robust governance to safeguard the interest of their investors. This includes performing proper due diligence before undertaking investments and addressing concentration and other risks to investors.

HOW CAN BDO HELP?

BDO Financial Services Group comprises a multi-disciplinary professional team with the right industry and subject matter expertise to meet your needs. We serve clients in the financial services sector, offer a wide range of services, including:

- Statutory Audit for Financial Institutions
- Regulatory and Compliance Advisory
  - Develop and implement a robust regulatory and compliance framework
  - Develop policies and procedures
  - Perform gap analysis of existing policies and procedures
  - Perform a regulatory health check on key business areas
  - Assist in license applications
  - Perform compliance outsourcing function
  - Provide training on new/revised regulations which will impact you
  - Assist in the implementation and on-going compliance with the Foreign Account Tax Compliance Act, Personal Data Protection Act and Anti-Money Laundering requirements
- Corporate Governance and Risk Management Services
- Internal Audit and Control Framework

www.bdo.com.sg

CONTACTS

TEI TONG HUAT Partner	tonghuat@bdo.com.sg	+65 6828 9181
GABRIEL SEOW Partner	gabrielseow@bdo.com.sg	+65 6828 9182
ADELINE TOH Director	adelinetoh@bdo.com.sg	+65 6829 9611
GRACE FOO Manager	gracefoo@bdo.com.sg	+65 6829 9623

This newsletter has been prepared for general guidance on matters of interest only, and does not constitute professional advice. It does not take into account any objectives, financial situation or needs of any recipient; any recipient should not act upon the information contained in this newsletter without obtaining independent professional advice. No representation or warranty (express or implied) is given as to the accuracy or completeness of the information contained in this newsletter and, to the extent permitted by law, BDO, its members, employees and agents do not accept or assume any liability, responsibility or duty of care for any consequences of you or anyone else acting, or refraining to act, in reliance on the information contained in this newsletter or for any decision based on it.

BDO LLP is a member of BDO International Limited, a UK company limited by guarantee, and forms part of the international BDO network of independent member firms.

BDO is the brand name for the BDO network and for each of the BDO Member Firms.

©2021 BDO LLP. All rights reserved.

CONNECT WITH US.