Issue 01/2022
www.bdo.com.sg

Newsletter

Regulatory Updates for Fund Management Companies

Welcome to the first newsletter of the BDO Regulatory Updates for Fund Management Companies for the Year 2022. This newsletter serves as a summary of the key regulatory developments for fund management companies or capital markets services licensees covering the period from 1 November 2021 to 30 June 2022.

CONTENTS

REGULATORY DEVELOPMENTS

From 1 November 2021 to 30 June 2022, the authorities of Singapore have issued or updated a series of Notices, Guidelines, Advisory and Consultation Papers.

Consultation Paper on Proposed Changes to the Complex Products Regime for Retail Investors

Status	First Issue Date: **3 November 2021** Effective Date: -

- On 3 November 2021, the Monetary Authority of Singapore ("MAS") issued a consultation paper on proposed changes to the classification of certain investment products as complex products entailing enhanced safeguards when distributed to retail investors.
- MAS also proposed changes to increase retail investors' access to diversified investment funds. The consultation closed on 15 December 2021.
- The objective of the complex products regime is to aid retail investors in better understanding the features and risks of a complex product before transacting in a complex product.
- MAS prescribes a list of products which are well-established in the market and have terms and conditions generally understandable by the market, termed Excluded Investment Products ("EIPs"). Products that do not fall within the prescribed list of EIPs are regarded as more complex products, also referred to as Specified Investment Products ("SIPs") and must be sold with enhanced distribution safeguards. These safeguards include requiring intermediaries to assess a customer's investment knowledge and experience before allowing the customer to transact in a SIP.

- The proposals relate to the EIP/SIP classification of collective investment schemes, debentures, perpetual securities and preference shares, and the distribution safeguards that apply to the sale of SIPs, as summarised below:

Type of products	Proposed changes
Collective Investment Schemes ("CIS")	▶ To classify as EIPs all authorised and recognised CIS (and correspondingly investment-linked policies ("ILP") sub-funds that invest in authorised/recognised CIS), except for a small group of more complex funds, to make it easier for retail investors to invest in diversified and professionally managed funds, including exchange traded funds (ETFs). ▶ Complex funds are those that employ alternative investment strategies, or embed unique features not typically encountered in traditional funds, and such funds are currently subject to additional disclosure requirements. MAS is of the view that such complex funds should continue to be classified as SIPs and subject to enhanced distribution safeguards as retail investors may be less familiar with them and more likely to require prior financial knowledge or experience to be able to understand the investment risks.
Debentures	▶ To classify debentures with the following features as SIPs: a. The interest payment is not solely based on a single fixed or floating rate, e.g., where the return is dependent on the performance of a defined asset pool and; b. The debentures are convertible, e.g., where the debt may be converted to equity. ▶ The reason for this proposal is because most retail investors with no prior financial knowledge or experience in dealing with such investment products may commonly understand debentures as an instrument that promises the return of principal with regular interest payment and may not fully appreciate the added complexity of debentures with such features.
Perpetual Securities and Preference Shares	▶ To classify perpetual securities as SIPs instead of the current EIP classification or to further assist retail investors to better understand the features and unique risks of perpetual securities e.g., disallowing perpetual securities from being marketed or described as bonds, requiring the inclusion of cautionary statements in advertising material that highlight the key features and risks of perpetual securities. ▶ MAS is also seeking comments on whether to align the EIP/SIP classification of preference shares with that of perpetual securities given the similarities between preference shares and perpetual securities (e.g., no obligation to repay the principal) and how they are often thought of as similar products. Preference shares are currently classified as EIP.

Circular on Non-face-to-face Customer Due Diligence Measures for Financial Institutions

Status	First Issue Date: **8 February 2022** Effective Date: **8 February 2022**

- On 8 February 2022, the Monetary Authority of Singapore ("MAS") issued a circular on Non-face-to-face Customer Due Diligence Measures ("Circular") which sets out industry good practices observed by MAS and supervisory guidance on the measures to mitigate risks associated with the use of non-face-to-face ("NFTF") technologies for customer due diligence ("CDD").

- The key guidelines are set out as follows:

a. ***Non-face-to-face Customer Due Diligence Measures***

	Non-face-to-face Customer Due Diligence Measures
Natural Persons	▶ Where financial institutions ("FIs") have utilized video conferencing as a means to onboard customers instead of physical meeting, they should implement the following: a. Putting in place appropriate controls during the video-conferencing process to verify the identity of the customer and the authenticity of the identification ("ID") documents sighted via video conferencing to mitigate risks of fraud and impersonation (e.g., use of control questions to be answered by the customer, or performance of liveness checks); b. Continuing to raise staff vigilance and conducting training to enable detection of possible fraudulent or tampered ID documents; and c. Performing additional checks via a different channel as appropriate, especially for accounts with higher money laundering and terrorism financing ("ML/TF") risks (e.g., verifying the customer's information against reliable and independent databases or performing a check sum digit test to identify data validation errors in the customer's ID document).

	Non-face-to-face Customer Due Diligence Measures
Legal Persons and Legal Arrangements	▶ CDD documents that cannot be verified against a registry or lack the requisite authenticity markers (such as a foreign certificate of incorporation) should not be verified purely via video conferencing. ▶ FIs should institute additional measures to verify that the soft copies of documents are genuine, such as by obtaining an original certified true copy or requiring suitably qualified persons to use digital signatures or watermarks to certify the authenticity of the soft copies. ▶ FIs should assess the robustness of processes in place to safeguard the authenticity of electronic documents and their admissibility in court.

b. ***Use of New Technology Solutions***

	Use of New Technology Solutions
Risk of Impersonation	▶ MAS notes that most solutions deployed by FIs surveyed included elements of biometrics technology, such as facial recognition. ▶ Liveness detection technology is also employed to verify if the FI is interfacing with an actual customer or a fake representation.
Risk of Fradulent or Tampered Documents	▶ When using in-house or third-party ID document authenticity verification tools to detect fraudulent or tampered ID documents, the following should be set in place by the FIs: a. Conducting an internal assessment of the effectiveness of the solutions in mitigating impersonation and fraud risks prior to implementing them; b. Not solely relying on external quality assurance standards of the technology service providers to arrive at their conclusion, but instead performing their own assessments; c. Assessment of technology solutions should be approved by board and senior management.
Enhancing Internal Controls	▶ MAS notes that technology solutions used to improve onboarding efficiency and mitigate risks associated with NFTF onboarding are not immune to failures and can still be exploited by criminals. ▶ When verification by the new technology solution fails, corrective action is required. It is important for FIs to establish appropriate metrics to monitor the performance of the technology solutions employed and take timely intervention measures where there are issues observed. ▶ The board and senior management of FIs are expected to maintain effective oversight of the management of ML/TF risks and anti-money laundering and countering the financing of terrorism controls. ▶ FIs should put in place effective mitigating controls to address the heightened impersonation and fraud risks where customers are onboarded remotely. ▶ FIs should also properly establish clear accountability for the effectiveness of NFTF CDD processes and technology solutions to manage these risks.

Notice SFA 04-N02 to Capital Markets Intermediaries on Prevention of Money Laundering and Countering the Financing of Terrorism

Status	First Issue Date: **24 April 2015** Revision Date: **1 March 2022** Effective Date: **1 March 2022**

▶ On 1 March 2022, the Monetary Authority of Singapore ("MAS") amended the AML/CFT rules to include Digital Capital Market Products ("CMP") token transactions and value transfers.

▶ MAS also made some revisions to the Customer Due Diligence section and all Capital Market Intermediaries ("CMI") should be aware of MAS' expectations.

- The table below sets out the significant changes to Notice SFA 04-N02 ("the Notice"):

Digital CMP token transactions	▶ A CMI shall perform CDD measures and screening when the CMI undertakes any digital CMP token transactions for any customer who has not otherwise established business relations with the CMI. ▶ On an ongoing basis, the CMI shall perform enhanced risk mitigation measures, except where the customer is a FI as defined in S27A(6) of the MAS Act or an overseas FI subject to and supervised for compliance with AML/CFT requirements consistent with standards set by the Financial Action Task Force ("FATF"). ▶ Digital CMP token, as defined in the Notice, means a digital representation of a capital markets product which can be transferred, stored or traded electronically.
Value transfers	▶ A CMI shall perform CDD measures and screening when the CMI effects or receives digital CMP tokens by value transfer, for a customer who has not otherwise established business relations with the CMI. ▶ Value transfer, as defined in the Notice, refers to any transaction carried out on behalf of a value transfer originator through a financial institution with a view to making one or more digital CMP tokens available to a beneficiary person at a beneficiary institution, irrespective of whether the originator and the beneficiary are the same person. ▶ MAS has added a new section 10A Value Transfers in Notice SFA04-N02 which lists the responsibilities of the Ordering Institution, the Beneficiary Institution and the Intermediary Institution.
Customer due diligence	▶ Where the CMI – a. has assessed that the money laundering and terrorism financing risks in relation to the customer are not high; and b. is unable to obtain the unique identification number of the connected party after taking reasonable measures, the CMI may obtain the date of birth and nationality of the connected party, in lieu of the unique identification number. The CMI shall document the results of the assessment and all the measures taken. ▶ Where the CMI – a. has assessed that the money laundering and terrorism financing risks of the customer are not high; and b. is unable to obtain the residential address of the natural person who acts or is appointed to act on behalf of the customer after taking reasonable measures, the CMI may obtain the business address of this natural person, in lieu of the residential address. The CMI shall take reasonable measures to verify the business address using reliable, independent source data, documents or information, as well as document the results of the assessment and all the measures taken. ▶ Where a customer is a legal person for which the CMI is not able to establish if it has any – a. ongoing, apparent or visible operation or business activity; b. economic or business purpose for its corporate structure or arrangement; or c. substantive financial activity in its interactions with the CMI, the CMI shall assess whether any such customer presents a higher risk for money laundering or terrorism financing.

Consultation Paper on Revised Notices on Reporting of Misconduct of Representatives and Broking Staff

Status	
	First Issue Date: **July 2018**
	Revision Date: **19 April 2022**
	Effective Date: **-**

- On 19 April 2022, the Monetary Authority of Singapore ("MAS") issued a consultation paper on "Revised Notices on Misconduct Reporting Requirements under the Financial Advisers Act, Insurance Act and Securities and Futures Act".
- The consultation closed on 20 May 2022.
- MAS is consulting on revisions to the FAA-N14 Notice on Reporting of Misconduct of Representatives by Financial Advisers ("FAA Notice"), MAS 504 Notice on Reporting of Misconduct of Broking Staff by Insurance Brokers ("IA Notice") and SFA 04-N11 Notice on Reporting of Misconduct of Representatives by Holders of Capital Markets Services Licence and Exempt Financial Institutions ("SFA Notice") (collectively, "Revised Notices") to implement changes to the misconduct reporting requirements.
- MAS will be making the following key changes to the misconduct reporting requirements:
  a. Application of the revised IA Notice to accident and health insurance intermediaries;
  b. Application of the revised SFA Notice to Registered Fund Management Companies (RFMCs);
  c. Revisions to the categories of reportable misconduct;

d. Revision to the reporting timeline of the misconduct report (and subsequent updates to the misconduct report) which the FI is required to submit to MAS;
e. Requirement for FIs to submit to MAS an investigation report (where the FI has commenced an internal investigation into the alleged misconduct) at the same time the FI submits a misconduct report to MAS;
f. Requirement for FIs to submit to MAS a copy of any report lodged with the police (where available), with accompanying information as set out in the Revised Notices at the same time the FI submits a misconduct report to MAS; and
g. Requirement for FIs to provide their representatives with a copy of the misconduct report (including subsequent updates to the misconduct report) filed with MAS within the timeline set out in the Revised Notices.

- FIs will be required to submit misconduct and investigation reports using prescribed formats.
- MAS will inform the industry of the effective date of the Revised Notices in due course and provide an adequate transition period for FIs to comply with the Revised Notices.

Information Papers on Environmental Risk Management for Banks, Asset Managers and Insurers

Status	First Issue Date: **31 May 2022** Effective Date: **-**

- On 31 May 2022, the Monetary Authority of Singapore ("MAS") published information papers on environmental risk management for banks, insurers and asset managers which provide an overview of the progress made in the implementation of the MAS Guidelines on Environmental Risk Management.
- The information papers are based on a thematic review conducted by MAS in 2021 on selected financial institutions ("FIs") and highlight emerging and/or good practices by them while identifying areas where further work is needed.
- The information papers also serve as a reference for these FIs as they continue to strengthen their resilience to environmental risk.
- A summary of the information paper for asset managers is set out below:

	Information Paper on Environmental Risk Management ("ENRM")
Asset Managers	▶ MAS conducted a survey of 30 selected asset managers ("AM") in 2021 ahead of the effective date of the ENRM Guidelines to assess the pace of implementation and to benchmark practices. ▶ Survey responses showed mixed progress across the AMs, and the positive observations include the following: a. Most AMs recognised the relevance and urgency of environmental risk and had put in place frameworks, governance arrangements and policies to oversee this risk; b. Public commitments to sustainable investing were also made by many AMs; c. Staff with relevant expertise to lead sustainable finance efforts had been hired, while internal staff were trained, and relevant third-party data was procured to supplement the internal assessment of environmental risk; and d. Some AMs had begun to make sustainability-related disclosures to share how they manage environmental risk while delivering long-term value to their stakeholders. ▶ Significant work still remains for the AMs to meaningfully incorporate environmental risk management practices in their firms such as having clear quantitative targets over different time horizons and embedding top-down/ bottom-up environmental risk assessment across all asset classes, strategies and portfolios.

Revised Business Continuity Management Guidelines for Financial Institutions

Status	First Issue Date: **June 2003** Revision Date: **6 June 2022** Effective Date: **Within 12 months following revision date**

- On 6 June 2022, the Monetary Authority of Singapore ("MAS") issued a revised version of the Business Continuity Management Guidelines ("Guidelines") to help financial institutions ("FIs") strengthen their resilience against service disruptions arising from IT outages, pandemic outbreaks, cyber-attacks and physical threats.
- To enable the continuous delivery of services to customers, FIs should adopt a service-centric approach through timely recovery of critical business services facing customers, identify end-to-end dependencies that support critical business services and address any gaps that could hinder recovery of such services, and enhance threat monitoring and environmental scanning, and conduct regular audits, tests, and industry exercises.
- Senior management of the FIs and personnel who are responsible for implementing business continuity management ("BCM") are expected to familiarize themselves with the Guidelines and understand their intent and implications.

- A brief overview of the revised Guidelines is set out below:

Effective date of the Guidelines	▶ FIs are expected to meet the Guidelines within 12 months of the issuance of the Guidelines. ▶ FIs should establish their BCM audit plan within 12 months and the first BCM audit should be conducted within 24 months of the issuance of the Guidelines.
Critical business services and functions	▶ FIs should prioritise the recovery of their business services and function based on their criticality and determine the appropriate recovery strategies and resource allocation. ▶ FIs should identify their critical business services and functions by considering the impact of the unavailability on the following factors: a. FI's safety and soundness b. FI's customers c. Other FIs that depend on the business service ▶ FIs should review their critical business services and functions at least annually, or whenever there are material changes to the people, process, technology, or other resources that support the delivery of critical business services. ▶ To minimize the degree of disruption, safeguard customer interests and maintain the safety and soundness of the FI, FIs establishing recovery strategies should adopt an end-to-end view of the critical business services' dependencies while considering the recovery of the complete set of processes supporting the delivery of the service. ▶ FIs should appoint personnel to oversee the recovery and resumption of each critical business service in the event of a disruption for clear accountability and responsibility for the business continuity of critical business services.
Service Recovery Time Objective (SRTO)	▶ FIs should establish a Service Recovery Time Objective ("SRTO") for each critical business service and implement recovery strategies to meet the SRTOs. ▶ When establishing SRTOs, FIs should consider their obligations to customers and other FIs that depend on the business services. ▶ FIs are further expected to put in place recovery strategies to achieve the established SRTOs and recover to the service levels required to meet their business obligations. ▶ For critical business services that are supported by a number of business functions, FIs must ensure that the Recovery Time Objectives ("RTOs") of the underlying business functions and their dependencies will meet the SRTOs. ▶ Clear and defined criteria should also be set out for activation of business continuity plans ("BCP") in the event the performance of a critical business service is reduced or intermittent, before it is completely unavailable.
Dependency mapping	▶ Dependency mapping is done on the following two fronts: 1. People, processes and technology - FIs should identify and map the end-to-end dependencies on people, processes, technology and other resources (such as data) and consider the implications of their unavailability and address any gaps that could hinder the effectiveness and safe recovery of the critical business services. - Information derived from the dependency map should be used to verify that the recovery of the business functions and their dependencies can meet the established SRTOs. 2. Third-party dependencies - FIs should put in place measures that enable third parties to meet the SRTOs of its critical business services as the operational risk arising from the failure, delay or compromise of the third parties in providing the services is higher. - Examples of these measures include establishing and regularly reviewing operational level or service level agreements with third parties that set out specific and measurable recovery expectations and support the FI's BCM. - There should also be plans and procedures in place to address unforeseen disruptions, failure or termination of third-party arrangements, to minimise the impact of such adverse events. - FIs should also have measures in place to address disruption of common utility services (e.g., telecommunications networks and power utilities), such as implementing redundancy or alternative contingency arrangements.

Concentration risks	▶ Concentration risk may arise from the concentration of people, technology or other required resources in the same zone. ▶ An FI may also be exposed to concentration risk when several of its critical business services and/or functions are outsourced to a single service provider. ▶ Several approaches are set out in the Guidelines to mitigate the risk of concentration e.g., separating primary and secondary sites of critical business services and functions, or infrastructure (such as data centres) into different zones to mitigate wide-area disruption, and having cross-border support or alternative service providers as a contingency. ▶ FIs should be cognisant of the resultant risks from the implementation of alternate work arrangements to mitigate the risk of disease transmission at workplaces, which may entail changes to policies, operational processes, and use of equipment or IT systems that pose new operational risks and other challenges. FIs should put in place mitigating controls to address such new risks and challenges.
Continuous review and testing	▶ FIs should implement the following measures to address operational risks posed by both the latest and plausible future threats: - Embed BCM into their business-as-usual operations and establish BCPs that address a range of severe and plausible disruption scenarios which may evolve over time. - Actively monitor and identify external threats and developments that could disrupt their normal operations and have an escalation process to alert internal stakeholders and senior management in a timely manner. - Perform a review to identify areas of improvement and address gaps in their BCM measures following an operational disruption. - Update their BCM policies, plans, and procedures, including relevant training programmes for staff and test plans, based on changes in its operational environment and the threat landscape. - Review their critical business services and functions, their respective SRTOs/ RTOs and dependencies at least annually, or whenever there are material changes that affect them. - Conduct regular and comprehensive testing to validate their BCM preparedness.
Audit	▶ FIs should ensure their audit programs adequately cover the assessment of BCM preparedness based on the level of operational risks that they are exposed to, as BCM audits provide FIs with independent assessment of the adequacy and effectiveness of their BCM framework. ▶ An audit of the FI's overall BCM framework and the BCM of each of its critical business services should be conducted at least once every three years by a qualified party with the requisite BCM knowledge and expertise, who is independent of the unit or function responsible for the BCM of the FI. ▶ Processes to track and monitor the implementation of remedial actions in response to the audit findings should be established. ▶ Significant audit findings on lapses that may have severe impact on the FI's BCM should be escalated to the Board and senior management, and the FI should submit the BCM audit reports to MAS upon request.
Responsibilities of Board and senior management	▶ The Board and senior management are ultimately responsible for the FI's business continuity and should provide the leadership and strategic direction to establish strong governance over the FI's BCM. ▶ The senior management should provide an annual attestation to the Board on the state of the FI's BCM preparedness, the extent of its alignment with the Guidelines, and key issues requiring the Board's attention such as significant residual risk. ▶ The attestation should also be provided to MAS upon request.

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 6990 2804
GABRIEL SEOW Partner	gabrielseow@bdo.com.sg	+65 6990 2805
ADELINE TOH Director	adelinetoh@bdo.com.sg	+65 6990 2818

CONNECT WITH US.