INVESTMENT MANAGEMENT
ASSOCIATION OF SINGAPORE

BAKER & MCKENZIE.WONG & LEOW

IMAS Regulatory Roundup - "Outsourcing, Technology and Data Protection – How does it impact fund management companies?"

IMAS Seminar 20 January 2015

Ken Chia

Agenda

- New updates
  - MAS Circular on System Vulnerability Assessments and Penetration Testing – May 2014
  - MAS Circular on IT security risks posed by personal mobile devices – September 2014
  - MAS consultation exercise on Notice and Guidelines on Outsourcing – September 2014
- MAS Notice On Technology Risk Management
- PDPA and MAS Amendments to Notices on Prevention of Money Laundering and Countering the Financing of Terrorism

MAS outsourcing and technology updates

MAS Circular on System Vulnerability Assessments and Penetration Testing - Circular No. SRD TR 01/2014 21 May 2014

- As vulnerability assessments and penetration testing would only enable FIs to identify security deficiencies in their IT systems at a particular point in time, FIs should institute a robust regime of prompt system patching and hardening, as well as adopt secure software coding practice.
- Where an outsourcing arrangement involves the handling of sensitive customer data by the service provider, FIs shall ensure that the data is accorded the same level of protection as if it is processed in-house. Where applicable, stringent requirements for regular vulnerability assessments and penetration testing must be applied to the service providers' environment

MAS Circular on IT security risks posed by personal mobile devices - Circular No. SRD TR 02/2014 26 Sep 2014

- FIs must conduct a comprehensive risk assessment on BYOD implementation to ensure that measures adopted sufficiently mitigate the security risks associated with “Bring Your Own Device” (BYOD)
  - Impingement of privacy and personal use, Diverse device portfolio, Lack of control over device updates, Maturity of Mobile Security Solutions
- Consider common ways to address BYOD Security such as use of Mobile Device Management and Virtualisation solutions
- Regular vulnerability assessment and penetration testing must be carried out on the BYOD infrastructure to ensure that any security gaps are identified and rectified promptly.

MAS Outsourcing Notice and Guidelines

- As with TRM, the new Outsourcing Notice will be binding
  - defines a set of minimum standards for outsourcing management
  - sets out requirements for the assessment of service providers, access to information, conduct of audits on a service provider, protection of customer data, and termination of and exiting from an outsourcing arrangement.

Notice v Guidelines

- Notice
  - Material Outsourcing Arrangements
    - minimum standards
    - early termination
  - Protection of Customer Data
  - Outsourcing to overseas regulated financial institutions
- Guidelines
  - Parts also apply to non-material outsourcings

Noitice - Material Outsourcings

- Policies and processes to identify material outsourcing arrangements
- Adequate risk management framework, systems, policies and processes to assess, control and monitor
- Ensure continued compliance
- Central register of all material outsourcing arrangements
- Maintain adequate documentation and furnish to MAS on request

Guidelines – Material outsourcings

- Additional factors to consider
  - impact should service provider.. encounter a breach of security, confidentiality or compromise of customer information;
  - impact on the institution‘s customers, should the service provider fail to perform the service or encounter a breach of security or confidentiality
  - cost of outsourcing failure, which will require in-sourcing or seeking similar service from another service provider, as a proportion of total operating costs of the institution;

Guidelines

- Additional examples of Outsourcings
  - white-labelling arrangements such as for trading and hedging facilities
  - information systems hosting (e.g., software-as-a-service, platform-as-a-service, infrastructure-as-a-service);
  - management of policy issuance and claims operations by managing agents
  - support services related to archival and storage of data and records

Notification Of Adverse Developments

- New Guidelines
  - notification of any event that could potentially lead to prolonged service failure or disruption
  - alternative arrangements or reintegration if
    - An institution fails or is unable to demonstrate a satisfactory level of understanding of the nature and extent of risks involved or emerging from the outsourcing arrangement;
    - The confidentiality of its customer information cannot be assured.

Guidelines - Responsibility Of The Board

- Added responsibilities
  - setting a suitable risk appetite to define the nature and extent of risks that the institution is willing and able to assume from its outsourcing arrangements;
  - ensuring that senior management establishes appropriate governance structures and processes for sound and prudent risk management, including a management body that reviews controls for consistency and alignment with a comprehensive institution-wide view of risk

Guidelines - Responsibility of Senior Management

- Added responsibilities
  - ensuring that staff in the institution are made aware of these policies and procedures for its outsourcing arrangements;
  - regularly reviewing .. standards .. to reflect changes in the institution‘s overall risk profile and risk environment
  - monitoring and maintaining effective control of all risks from its material outsourcing arrangements on an institution-wide basis
  - ensuring appropriate and timely remedial actions are taken to address audit findings

Guidelines – other points

- self assessment within 2 months if become regulated or if M&A

- track record of service provider will need to be considered
- FI specific audits and metrics required (i.e. not aggregated with metrics or data belonging to other customers of the service provider)
- indemnification of MAS for inspections and audits

Circular No. SRD TR 01/2014
21 May 2014

PDPA updates

PDPA does not affect other laws

- PDPA sets out minimum standards; additional sector-specific requirements will continue to apply
- PDPA does not affect any authority, right, privilege or immunity conferred, or obligation or limitation imposed, under the law
  - Performance of contractual obligation not excuse for contravening PDPA
  - Cannot claim to be exempt from compliance with PDPA when performing a contractual obligation
- Provisions of other written law prevail over PDPA to the extent inconsistent
- Law vs written law? Includes directions, codes of practice, licence conditions, guidelines, common law?

Application to banking disclosures

- Disclosures required under written law (e.g. Corruption, Drug Trafficking and Other Serious Crimes (Confiscation of Benefits) Act or CDSA)
- Disclosures required under AML/CFT notices issued by MAS
- Disclosures required for compliance with laws of other jurisdictions (e.g. SDR under Dodd-Frank Act, FACTA)
  - Is personal data disclosed?
  - Is disclosure exempted under Third Schedule of Banking Act?
- NB: Disclosure in connection with the promotion of financial products and services to customers of any licensed financial institution deleted

Other potential areas of overlap

- Collection of personal data for KYC
- Guidelines on outsourcing/ cloud computing
- Technology risk management

Regulatory actions taken by MAS

- MAS Amendments to Notices on Prevention of Money Laundering and Countering the Financing of Terrorism
  - Consultation Paper on Obligations of Financial Institutions under the Personal Data Protection Act 2012 issued 2 Jun 2014
  - Amendments effective 2 July 2014

Key points

- no need for consent for collection, use and disclosure of personal data to comply with Notice
  - of an individual customer
  - of someone appointed to act on behalf of a customer
  - of an individual beneficial owner of a customer

Key points

- Access and correction right only in relation to
  - a) full name, including any alias; (b) the unique identification number (such as an identity card number, birth certificate number or passport number); (c) the existing residential address and contact telephone number(s); (d) the date of birth; (e) the nationality; and
  - (f) any other personal data of the respective individual provided by that individual to the [FI]
- No need to provide access, info on use and disclosure or right to correct any other information in possession or control of FI

Questions ?

Ken Chia
Principal
Baker & McKenzie.Wong & Leow
8 Marina Boulevard
#05-01 Marina Bay Financial Centre Tower 1
Singapore 018981
Direct: +65 6434 2558
Main: +65 6338 1888
Fax: +65 6337 5100
ken.chia@bakermckenzie.com
www.bakermckenzie.com