



Circular No. SRD TR 01/2011

14 July 2011

The Chief Executive Officers of All Financial Institutions  
The Principal Officers of All Insurers

Dear Sir / Madam

## **INFORMATION TECHNOLOGY OUTSOURCING**

Outsourcing comes in many forms, shapes and permutations. In particular, some of the most common types of outsourcing are in IT and business processing functions ranging from systems development, maintenance and support to data centre operations, network administration, disaster recovery services, application hosting and cloud computing. These activities can involve the provision of IT capabilities and facilities by a single third party or multiple vendors located in Singapore or abroad.

2 Financial institutions are reminded that the responsibilities for effective due diligence, oversight and management of outsourcing and accountability for all outsourcing decisions continue to rest with the institution, its board and senior management. The financial institution should put in place proper framework, policies and procedures to evaluate, approve, review, control and monitor the risks and materiality of all its outsourcing activities.

3 Outsourcing in any configuration or at any location should not result in any weakening or degradation of a financial institution's internal controls. A financial institution should ensure that a service provider employs a high standard of care and diligence in its security policies, procedures and controls to protect the confidentiality and security of its sensitive information, such as customer data, computer files, records, object programs and source codes.

4 In the case of cloud computing, financial institutions should be aware of unique attributes and risks especially in the areas of data integrity, recoverability and confidentiality as well as legal issues such as regulatory compliance and auditing. In particular, as cloud computing service providers typically process data for multiple customers, financial institutions should pay attention to the service providers' ability to isolate and clearly identify their customer data and other information system assets for protection. In the event of contract termination with a service provider, either on expiry or prematurely, the financial institution should have the contractual power and means to have all such IT information and assets promptly removed or destroyed. Financial institutions should also consider the resiliency and safety of the service provider's infrastructure to ensure that their business continuity preparedness is not compromised by outsourcing.

5 Prior to entering into a contract with any outsourcing service providers, financial institutions should perform a thorough risk assessment of the proposed outsourcing arrangements against all relevant MAS regulations, guidelines and other requirements such as the MAS Guidelines on Outsourcing, Internet Banking & Technology Risk Management Guidelines, Notice 634 and Circular on Endpoint Security and Data Protection. Financial institutions can refer to the MAS Technology Questionnaire for Outsourcing for further guidance. This questionnaire is available on MAS' website<sup>1</sup>. Financial institutions are also required to consult and submit the completed questionnaire to MAS before making any significant<sup>2</sup> IT outsourcing commitment.

6 Should you have any questions or comments, please contact Mr Roy Teo, Head - Technology Risk Supervision at 6229 9174 or royteo@mas.gov.sg.

Yours faithfully

(via MASNET)

WAN AIK CHYE  
DIRECTOR & HEAD  
SPECIALIST RISK DEPARTMENT

---

<sup>1</sup> [http://www.mas.gov.sg/legislation\\_guidelines/risk\\_mgt/Guidelines\\_on\\_Risk\\_Management\\_Practices.html](http://www.mas.gov.sg/legislation_guidelines/risk_mgt/Guidelines_on_Risk_Management_Practices.html)

<sup>2</sup> Outsourcing involving customer personal or account data, transactions, deposits, loans, payment card data, trading details and investment portfolios is generally considered as significant.