



Circular No. SRD TR 02/2010

30 July 2010

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

Dear Sir / Madam

INFORMATION SYSTEMS RELIABILITY, RESILIENCY AND RECOVERABILITY

Information technology is a key enabler for the business operations and market activities conducted by financial institutions. The reliability, availability, and serviceability of IT systems, networks and infrastructures are crucial in maintaining confidence and trust in the operational and functional capability of financial institutions. When mission-critical systems fail, the disruptive impact on a financial institution's operations and functions will usually be immediate, severe and widespread, with serious consequences to its reputation.

2 The board of directors and senior management of financial institutions are fully responsible for managing risks, including technology risks. At all times, MAS expects financial institutions to have effective internal controls and risk management practices which ensure the robustness, resiliency and recoverability of their IT systems and infrastructures.

3 In formulating and constructing a rapid recovery plan, contingency scenarios should envisage major system outages and the total incapacitation of the primary data centre. For critical systems, a recovery time objective of four hours or less should be established and maintained; stringent recovery point objectives that are commensurate with the financial institutions' business requirements should also be defined.

4 To strengthen recovery measures relating to large scale disruptions and to achieve risk diversification, financial institutions are expected to implement rapid operational and backup capabilities at the individual system or application cluster level. Financial institutions should ensure that inter-dependencies between critical systems are accounted for in their recovery plans and contingency tests.

5 The architecture and connectivity of disk storage sub-systems, particularly storage area networks (SAN) should be regularly reviewed for single points of failure and fragility in functional design and specifications, as well as technical support by service providers. As and when these risks are discovered, prompt remedial actions should be taken to resolve them. Sound patch management processes should also be instituted, where appropriate, to keep systems contemporaneous with new releases of microcode, firmware and software upgrade.

6 Outsourcing to service providers does not in any way diminish the responsibilities and accountabilities of financial institutions. The board and senior management of financial institutions retain full responsibility for managing risks and internal controls. Financial institutions that outsource material IT functions and operations should maintain effective oversight of all outsourced activities. MAS expects financial institutions to remain vigilant and monitor rigorously the status and health of all their critical applications, systems, devices and networks.

7 Financial institutions should adopt the sound principles and best practices contained in MAS' Internet Banking & Technology Risk Management Guidelines and Guidelines on Outsourcing taking into account the size, nature and complexity of their operations. Through its supervisory process, MAS will continue to assess the adequacy of financial institutions' risk management systems and controls, and the extent to which they have adopted MAS Guidelines.

8 Should you have any questions or comments, please contact Mr Tony Chew, Director, Technology Risk Supervision at 62299109 or tonychew@mas.gov.sg.

Yours faithfully

(via MASNET)

CHUA KIM LENG
EXECUTIVE DIRECTOR
SPECIALIST RISK DEPARTMENT