CONSULTATION PAPER

P013 - 2012

JUNE 2012

NOTICE ON TECHNOLOGY RISK MANAGEMENT

Monetary Authority of Singapore

PREFACE

MAS has issued various guidelines and circulars to the financial industry over the years to promote sound technology risk management and security practices. To further this effort, MAS is proposing to issue a Notice on Technology Risk Management that sets out the obligations of the financial institutions which include requirements relating to system recoverability and reliability, IT security incidents and major systems failure notification, as well as security of customer information.

MAS invites interested parties to submit their views and comments on the draft Notice. Electronic submission is encouraged. Please submit your comments by 16 July 2012 to:

Technology Risk Supervision Division
Specialist Risk Department
Monetary Authority of Singapore
10 Shenton Way, MAS Building
Singapore 079117
Email: techrisk@mas.gov.sg
Fax: 62299659

Please note that any submission received may be made public unless confidentiality is specifically requested for the whole or part of the submission.

TABLE OF CONTENTS

1 INTRODUCTION

1.1 The objective of issuing the Notice for Technology Risk Management is to require the financial institutions to manage their critical IT infrastructure and systems with high level of robustness and integrity; as well as implement adequate IT controls to protect customer information from unauthorised access or disclosure.

1.2 The reliability, availability, and recoverability of IT infrastructure and systems, are crucial in maintaining confidence and trust in the operational and functional capabilities of a financial institution. When critical systems that support essential business functions fail, the disruptive impact on the financial institution's operations and functions will usually be immediate, severe and widespread, with serious consequences to reputation. In this regard, the following requirements are proposed:

i. Financial institutions shall put in place a framework and process to identify critical systems.

ii. Financial institutions shall maintain high availability for critical systems where maximum allowable unscheduled downtime within 12 months shall not exceed 4 hours. To achieve high availability, financial institutions will have to enhance the resiliency of critical systems by building sufficient fault tolerance and redundancies in the IT infrastructures that support these systems.

iii. Financial institutions shall recover critical systems in 4 hours or less, in the event of a disaster. The recovery time objectives shall be documented and verified once every 12 months.

iv. Financial institutions shall inform MAS about all IT security incidents and major systems malfunction within 30 minutes upon discovery of the incidents. Financial institutions shall also submit a root cause and impact analysis report to MAS within one month from the occurrence of any IT security incident and major systems malfunction. This is to provide MAS with timely information on disruptive events relating to IT security as well as critical systems and IT infrastructure.

1.3 Data which are stored and processed electronically are susceptible to data loss, leakage or other forms of compromise through mishandling and other poor data

protection practices. To maintain the integrity of customer information, we are proposing that financial institutions implement IT controls to protect customer information from unauthorised access or disclosure.

2 DRAFT NOTICE ON TECHNOLOGY RISK MANAGEMENT

Notice No: MAS xxx

Issue Date: Xx xxx 2012

Technology Risk Management

Introduction

1 This Notice is issued pursuant to section 28(3) of the Monetary Authority of Singapore Act (Cap. 186) ("the Act").

2 This Notice applies to any financial institution.

Definitions

3 For the purpose of this Notice,

"critical system" means a system supporting essential business functions of the financial institution such that any failure will cause severe disruption to the financial institution's operations; and

"financial institution" has the same meaning as in section 27A(6) of the Act.

4 Any expression used in this Notice shall, except where expressly defined in this Notice or where the context requires, shall have the same meaning as in the Act.

Technology Risk Management

5 The financial institution shall put in place a framework and process to identify critical systems.

6 Financial institutions shall take all reasonable effort to maintain high availability for critical systems. The financial institution shall ensure that the maximum unscheduled downtime for its critical systems within 12 months does not exceed 4 hours.

7 The financial institution shall establish an RTO of 4 hours or less for its critical systems. RTO or recovery time objective means the time required to recover an IT

system starting from the point of disruption to the IT system involving any IT incident referred to in paragraph 8. The financial institution shall verify and document how and when the RTO is achieved at least once every 12 months.

8 The financial institution shall inform the Authority in writing within 30 minutes upon the discovery of all IT security incidents and major systems malfunction. An IT security incident means an event that involves security breaches, hacking, intrusion or compromise of customer data. Major systems malfunction means a failure of any of the financial institutions' critical systems, IT networks or IT applications.

9 The financial institution shall submit a root-cause and impact analysis report to the Authority within 1 month from the occurrence of any IT security incident and major system malfunction. The report shall contain an executive summary of the incident, an analysis of root causes which trigger the incident, the impact of the incident on regulations, operations and customers, legal and reputational implications, as well as remedial measures taken to address the consequences of the incident.

10 The financial institution shall implement IT controls to protect customer information from unauthorised access or disclosure.

Effective Date

11 This Notice shall take effect on [ ].