Monetary Authority of Singapore

RESPONSE TO FEEDBACK RECEIVED – CONSULTATION PAPER ON THE NOTICE ON TECHNOLOGY RISK MANAGEMENT

1 Introduction

1.1 On 13 June 2012, MAS conducted a consultation on the Notice on Technology Risk Management (the "Notice"). The proposed Notice sets out the obligations of the financial institutions ("FIs") which include requirements relating to system reliability, availability and recoverability, notification of IT security incidents and malfunction of critical systems, as well as the security of customer information.

1.2 The consultation closed on 16 July 2012 and we thank all respondents for their feedback and comments. As many respondents have requested for confidentiality, MAS will not be publishing the list of respondents.

2 Implications of Breaches to the Notice

2.1 One respondent enquired about the implications of breaches to the Notice.

MAS' Response

2.2 Separate Notices will be issued under the respective Acts which apply to FIs. FIs that fail to comply with any of the requirements will be in contravention of the provision of the Act under which the Notice is issued. The approach in which MAS treats a breach to the Notice will be consistent with that for other breaches of regulations.

3 Scope of Financial Institution and Applicability of the Notice

3.1 Some respondents enquired about the scope of "financial institution" as defined in the Notice.

3.2 Other respondents also enquired whether the Notice is applicable to a Branch office of an overseas FI.

3.3 Some respondents highlighted that different types of FIs have different operating models and enquired whether the same requirements should be applied across all FIs without taking into account the size, complexity and type of FIs. Some observed that the requirements can be onerous for smaller FIs.

MAS' Response

3.4 We have considered the feedback and refined the scope of "Financial Institutions" which are obliged to comply with the requirements in the Notice.

3.5 In addition, any FI, including a Branch office of an overseas FI that is licensed, approved, or otherwise regulated by MAS must comply with Singapore's laws and regulations. The requirements set in the Notice are applicable to all such FIs which rely on systems in its operations, even if such systems are outsourced.

3.6 The FIs to which the Notices apply are:

S/No.	FIs	Governing Act	Notice No.
1	All- (a) approved exchanges; (b) designated clearing houses; (c) holders of a capital markets services licence; (d) recognised market operators which are incorporated in Singapore; and (e) persons who are approved under section 289 of the Securities and Futures Act to act as a trustee of a collective investment scheme which is authorised under section 286 of the Securities and Futures Act and constituted as a unit trust	Securities and Futures Act	Notice CMG-N02
2	All licensed financial advisers	Financial Advisers Act	Notice FAA-N18
3	All licensed insurers, other than captive insurers and marine mutual insurers	Insurance Act	Notice MAS 127
4	All registered insurance brokers	Insurance Act	Notice MAS 506
5	All banks in Singapore	Banking Act	Notice MAS 644
6	All credit card or charge card licensees in Singapore	Banking Act	Notice MAS 762
7	All finance companies	Finance Companies Act	Notice MAS 830
8	All money brokers approved under section 28 of the Monetary Authority of Singapore Act	Monetary Authority of Singapore Act	Notice MAS 912
9	All merchant banks approved under section 28 of the Monetary Authority of Singapore Act	Monetary Authority of Singapore Act	Notice MAS 1114
10	All holders of a remittance licence issued under section 8 of the Money-changing and Remittance Businesses Act	Money-changing and Remittance Businesses Act	Notice MAS 3203
11	All operators and settlement institutions of designated payment systems	Payment Systems (Oversight) Act	Notice PSOA-N05
12	All trust companies licensed under the Trust Companies Act	Trust Companies Act	Notice TCA-N05

3.7 In deciding on the applicability of the Notice, MAS considered the size, complexity and type of FIs. In addition, MAS identified the areas and the

requirements for ensuring the robustness of critical systems and protecting customer information from unauthorised access or disclosure. The set of mandatory requirements should be applied consistently across the financial industry. MAS is aware that some FIs do not operate critical systems as defined in the Notice.

4 Similar Requirements in Different MAS Regulations and Guidelines

4.1 The respondents asked whether the requirements in this Notice supersede similar requirements and guidance in other MAS regulations and guidelines. The following examples are cited:

a) Sections 9 of the Securities and Futures (Market) Regulations and section 9 of the Securities and Futures (Clearing Facilities) Regulations, where FIs are required to submit incident reports to MAS within 14 days; and
b) Circular SRD BCM 01/2006, where FIs are expected to inform MAS' supervisory officers immediately of the occurrence of any emergency where business operations are or will be severely disrupted, as well as once their contingency plans have been activated.

MAS' Response

4.2 The requirements in the Notice do not supersede other circulars, guidelines, notices, regulations or Acts governed by MAS. Each FI should at all times ensure compliance with the provisions of the Acts and regulations which are applicable to it.

5 Definition of Critical Systems

5.1 Some respondents enquired on the definitions of and criteria for identifying: "critical systems" and "essential business functions" as used in the Notice.

5.2 Many respondents also proposed the following criteria for "critical systems":

a) Systems which in the event of failure will cause a material impact to the FI's operations and its customer base in Singapore;
b) Systems which process transactions that are time critical;
c) Systems which are essential for the conduct of customers' transactions, such as ATM, online banking and teller systems; and
d) Systems which support payment, settlement and clearing functions.

5.3 Some respondents asked whether IT networks, databases and application systems are considered as part of "critical systems".

MAS' Response

5.4 A "critical system" means a system, the failure of which will cause significant disruption to the operations of the FI or materially impact the FI's service to its customers. This includes systems which process transactions that are time critical, or provide essential services to customers. Systems listed in 5.2 would fall within the definition of critical systems.

As each FI is in a better position to understand the importance of their systems to their business, it is essential that the FI establishes a proper framework and process to assess and identify critical systems.

5.5 A "system" is any hardware, software, network or other IT component which is part of an IT infrastructure.

6 Unscheduled Downtime Requirement

6.1 Many respondents suggested defining the unscheduled downtime for critical systems in terms of the industry standard for scheduled system uptime in percentage. The respondents enquired whether the unscheduled downtime includes non-business operating hours.

6.2 Some respondents enquired whether the 4-hour unscheduled downtime requirement is computed on the basis of a single critical system or for all critical systems.

MAS' Response

6.3 The focus of the requirement is to ensure that the FI can recover its critical system swiftly during a Relevant Incident, as defined in the issued Notice on Technology Risk Management. The appropriate measure is expressed as unscheduled downtime in hours because system uptime expressed in the percentage form over a period may obscure the seriousness of a system failure at a particular point of time.

6.4 The 4-hour unscheduled downtime requirement applies to each critical system. For the avoidance of doubt, system downtime that is planned beforehand for activities such as system maintenance, upgrading or replacement is not considered as unscheduled downtime.

7 Exclusion from the Unscheduled Downtime Requirement

7.1 One respondent commented that critical systems which do not significantly impact external parties should be excluded from this requirement.

MAS' Response

7.2 Critical systems which do not significantly impact external parties may nonetheless cause significant disruption to the FI's operations. Hence, the FI must ensure compliance to the Notice for systems identified as "critical".

8 Clarification on the term "Reasonable Effort"

8.1 One respondent noted that FIs are required to make all reasonable effort to maintain high availability and sought clarification on the term "reasonable effort".

MAS' Response

8.2 MAS would expect an FI to ensure high availability for their critical systems, including examining its systems and controls, and implementing processes and procedures, to achieve resiliency for the FI's critical systems. FIs can refer to Chapter 8 of the Technology Risk Management Guidelines for more information.

9 Complying With 4 Hours Recovery Requirement

9.1 One respondent enquired whether there is a need to comply with the 4 hours recovery time objective if the FI does not deem any system in its IT environment as critical.

MAS' Response

9.2 FIs is required to establish a framework and process to identify critical systems, as defined in the Notice.

9.3 If a system assessed as "non-critical" by the FI fails and the failure causes a significant disruption to the FI's operations or materially impacts the FI's service to its customers, the FI would have breached the Notice if the recovery time objective for the system exceeds 4 hours.

10 Definition of Recovery Time Objective for Critical Systems

10.1 Some respondents asked MAS to clarify on the definition "Recovery Time Objective (RTO)". The respondents also enquired whether the RTO of 4 hours is applicable for recovery of critical systems during non-business hours.

MAS' Response

10.2 "Recovery Time Objective" is defined as the time taken to restore an IT system to the last known normal state, starting from the point of disruption to the point when the IT system is recovered. The recovery time of critical systems should not exceed the stipulated 4 hours, even if the system outage or failure occurred during non-business hours.

11 Assigning Recovery Time Objective of 4 hours or Less for Critical Systems

11.1 Many respondents commented that it will be too onerous for FIs to define RTO of 4 hours or less for their critical systems. The respondents asked whether an RTO of 4 hours is applicable for critical systems which do not support time-critical financial services.

11.2 Some respondents opined that the RTO for critical systems should be assessed by the nature of the business conducted by the FI and subjected to the service commitment made by the FI to its customers. The alternative arrangement provided by the FI to its customers in the event of a system malfunction should also be taken into consideration when determining the RTO for critical systems. In the event that FI has an effective way of servicing its customers through a well-defined

Business Continuity Plan (BCP), its critical system should be allowed to recover within a reasonable time objective instead of 4 hours.

MAS' Response

11.3 MAS agrees that each FI should perform its risk assessment and determine the system recovery and business resumption priorities. However, in the context of "critical systems" as defined in the Notice, FIs are required to implement an effective and swift recovery strategy for systems where a system failure will lead to a severe and widespread impact on its operations or materially impact the FI's customers. It is important that these systems can be quickly recovered so as to minimise adverse impact on the FI's operations and reputation; or in maintaining customer confidence.

11.4 If a system supports the FI's essential functions and in the event of failure does not cause significant disruption to the FI's operations or materially impact the FI's customers, the FI should assess whether the system should be identified as a "critical system".

12 Verifying Recovery Time Objective (RTO) of Critical Systems

12.1 One respondent asked how FIs should verify the RTO of critical systems.

MAS' Response

12.2 RTO of critical systems should be validated during testing of the disaster recovery plan where the actual system recovery time is compared against the RTO.

13 Notifying the Authority upon Discovery of IT Security Incidents and Critical Systems Malfunction

13.1 Many respondents commented that a 30 minutes notification limit is too short and requested MAS to allow institutions more time to notify MAS of IT security incidents and system malfunctions. They highlighted that each FI will require time to investigate and confirm that an IT incident has occurred. The time taken to complete the initial investigation will vary as it is dependent on a few factors such as the complexity and circumstances of the IT incident, and the time at which the incident has occurred. Some respondents also highlighted the difficulty in notifying MAS within 30 minutes, as systems can be managed at overseas locations i.e. Head Office, where an event may occur at non-business hours in Singapore.

13.2 Several respondents also asked whether the requirement applies to a system malfunction resulting from services provided by a third party such as telecommunications and power companies.

13.3 One respondent also asked whether the requirement applies during non-business hours in Singapore.

MAS' Response

13.4 The objective of the requirement is to provide sufficient lead time to MAS to assess the wider impact of the incident on the industry and the public, as well as to coordinate with FIs to provide responses to the stakeholders.

13.5 To balance the practical concerns of FIs and the objective of the requirement, MAS has extended the requirement for notification within 30 minutes to 1 hour upon discovery of a system malfunction or an IT security incident that has severe and widespread impact on the FI's operations, or materially impacts the FI's service to its customers. For critical systems hosted overseas, FIs are, likewise, required to notify MAS within 1 hour upon discovery of a system malfunction or an IT security incident. MAS expects FIs to work with their service providers to ensure that information is communicated on a timely basis.

13.6 MAS should be notified at all times of any system malfunction or IT security incident, as defined in the Notice, when the event has a severe and widespread impact on the FI's operations, or materially impacts the FI's service to its customers; even if it has occurred during non-business hours.

14 Definition of IT Security Incident and Types of IT Security Incidents to Report

14.1 The respondents suggested that "IT security incident" should be defined with greater granularity. Some respondents asked what type of IT security incidents should be reported to MAS as the impact of such incidents on the FI's operations or customers vary in magnitude. For instance, a computer virus outbreak on one personal computer against an outbreak on hundreds of personal computers.

MAS' Response

14.2 Each FI is required to inform MAS of any IT security incident which has a severe and widespread impact on the FI's operations, or materially impacts the FI's service to its customers. The IT security incident is defined as an event that involves a security breach, such as hacking, intrusion or denial of service attack on a critical system, or on a system which compromises the security, integrity or confidentiality of any customer information.

15 Reporting Critical System Malfunction

15.1 A respondent sought clarification on whether each FI is required to report an automatic failover of a critical system to its backup system when it has already implemented real-time replication of the critical system; and business functions are not affected by the incident.

MAS' Response

15.2 For the purpose of the Notice, FIs do not need to report an automatic failover of a critical system to its backup system within an hour if the incident does not have a severe and widespread impact on the FI's operations, or a material impact on the FI's service to its customers.

16 Submission of Root Cause Analysis and Impact Analysis Report within 1 Month

16.1 Many respondents commented that a 1-month time window is too short to facilitate a detailed analysis of the root cause and impact of an IT security incident or a critical system malfunction.

MAS' Response

16.2 We have considered the respondents' suggestions and reviewed similar requirements in other MAS regulations and guidelines. MAS has amended the requirement such that an FI shall submit the report within 14 days from the discovery of a system malfunction or an IT security incident. From past experience, FIs were able to furnish incident reports within 14 days from the date of incident discovery and confirmation. Notwithstanding, FIs can request MAS to extend the incident report submission deadline.

16.3 MAS may grant extensions on a case-by-case basis if MAS assesses the IT security incident or critical system malfunction to be complex in nature.

17 Implementing IT Controls to protect Customer Information

17.1 Several respondents asked how MAS assesses the adequacy of FIs' IT controls in protecting customer information from unauthorised access and disclosure.

MAS' Response

17.2 MAS will review IT controls, processes and procedures that are implemented by FIs at the data, system and application layers, including data loss prevention controls, user and privileged ID controls, systems and network security controls. These controls, processes and procedures should be effective against unauthorised access to customer information.

18 Issuance Date of the Notice

18.1 Many respondents asked when the Notice will take effect and requested that sufficient time be given to FIs to meet the requirements stipulated in the Notice.

MAS' Response

18.2 MAS understands that some FIs need the time and resources to meet the requirements stipulated in the Notice. Time will be given for FIs to assess, prepare and implement the necessary infrastructure, controls, processes and procedures to meet the requirements stipulated in the Notice. The Notice will take effect on 1 July 2014.