MAS Notice No.: FSM-N11

Notice to merchant banks in Singapore
Financial Services and Markets Act 2022

Issue Date: 9 May 2024

NOTICE ON TECHNOLOGY RISK MANAGEMENT

Introduction

1 This Notice is issued pursuant to section 29(1) of the Financial Services and Markets Act 2022 (the "Act") and applies to all merchant banks in Singapore ("Merchant Banks").

Definitions

2 For the purpose of this Notice—

"banking business" has the meaning given by section 2(1) of the Banking Act 1970;

"critical system" in relation to a Merchant Bank, means a system, the failure of which will cause significant disruption to the operations of the Merchant Bank or materially impact the Merchant Bank's service to its customers, such as a system which—

(a) processes transactions that are time critical; or
(b) provides essential services to customers;

"customer", in relation to a Merchant Bank, includes the Monetary Authority of Singapore or any monetary authority or central bank of any other country or territory, and any company which carries on a banking business, a merchant banking business or an investment banking business;

"customer information", in relation to a Merchant Bank, means —

(a) any information relating to, or any particulars of, an account of a customer of the Merchant Bank, whether the account is in respect of a loan, investment or any other type of transaction, but does not include any information that is not referable to any named customer or group of named customers; or

(b) deposit information;

"deposit information", in relation to a Merchant Bank, means any information relating to —

(a) any deposit of a customer of the Merchant Bank;

(b) funds of a customer under management by the Merchant Bank; or

(c) any safe deposit box maintained by, or any safe custody arrangements made by, a customer with the Merchant Bank, but does not include any information that is not referable to any named person or group of named persons;

"funds of a customer under management" means any funds or assets of a customer (whether of the Merchant Bank or any financial institution) placed with that Merchant Bank for the purpose of management or investment;

"IT security incident" means an event that involves a security breach, such as hacking of, intrusion into, or denial of service attack on, a critical system, or a system which compromises the security, integrity or confidentiality of customer information;

"merchant bank in Singapore" has the meaning given by section 2(1) of the Banking Act 1970;

"permitted business" has the meaning given by section 55Q of the Banking Act 1970;

"relevant incident" means a system malfunction or IT security incident, which has a severe and widespread impact on the Merchant Bank's operations or materially impacts the Merchant Bank's service to its customers;

"system" means any hardware, software, network, or other information technology ("IT") component which is part of an IT infrastructure;

"system malfunction" means a failure of any of the Merchant Bank's critical systems.

3 Except where defined in this Notice or if the context otherwise requires, the expressions used in this Notice have the same meanings as in the Act.

Technology Risk Management

4 A Merchant Bank must put in place a framework and process to identify critical systems.

5 A Merchant Bank must make all reasonable effort to maintain high availability for critical systems. The Merchant Bank must ensure that the maximum unscheduled downtime for each critical system that affects the Merchant Bank's operations or service to its customers does not exceed a total of 4 hours within any period of 12 months.

6 A Merchant Bank must establish a recovery time objective ("RTO") of not more than 4 hours for each critical system. The RTO is the duration of time, from the point of disruption, within which a system must be restored. The Merchant Bank must validate and document at least once every 12 months, how it performs its system recovery testing and when the RTO is validated during the system recovery testing.

7 A Merchant Bank must notify the Authority as soon as possible, but not later than 1 hour, upon the discovery of a relevant incident.

8 A Merchant Bank must submit a root cause and impact analysis report to the Authority, within 14 days or such longer period as the Authority may allow, from the discovery of the relevant incident. The report must contain—

(a) an executive summary of the relevant incident;

(b) an analysis of the root cause which triggered the relevant incident;

(c) a description of the impact of the relevant incident on the Merchant Bank's—

i. compliance with laws and regulations applicable to the Merchant Bank;

ii. operations; and

iii. service to its customers; and

(d) a description of the remedial measures taken to address the root cause and consequences of the relevant incident.

9 A Merchant Bank must implement IT controls to protect customer information from unauthorised access or disclosure.

Effective Date

10 This Notice shall take effect on 10 May 2024.