

Notice No : CMG-N02 (Amendment) 2018

Issue Date : 3 October 2018

NOTICE ON TECHNOLOGY RISK MANAGEMENT

Introduction

1 For presentational purposes, the amendments in this document are compared against the version of the MAS Notice CMG-N02 on the Technology Risk Management [Notice No. CMG-N02] issued on 21 June 2013 and last revised on 6 March 2014.

2 This document shall be interpreted as follows:

(a) Text which is coloured and struck through represents deletion which will not appear in the untracked version of CMG-N02 revised on 3 October 2018, which is published on MAS' website www.mas.gov.sg ("Published Version"); and

(b) Text which is coloured and underlined represents insertion which will appear in the Published Version.

3 The amendments reflected in this document shall take effect on 8 October 2018.

4 This document is to be used for reference only. In the event of discrepancies between the amendments in this document and the Published Version, the Published Version shall prevail.



Monetary Authority of Singapore

**SECURITIES AND FUTURES ACT
(CAP. 289)**

NOTICE ON TECHNOLOGY RISK MANAGEMENT

Notice No.: CMG-N02

Issue Date: 21 June 2013 [Last revised on ~~6 March 2014~~ October 2018]

NOTICE ON TECHNOLOGY RISK MANAGEMENT

Introduction

1 This Notice is issued pursuant to sections 46, 46ZK, 81R, 81SV, 101, 123ZZB and 293 of the Securities and Futures Act (Cap. 289) (the “Act”) and applies to all —

- (a) approved exchanges;
 - (aa) licensed trade repositories;
 - (b) approved clearing houses;
 - (ba) recognised clearing houses which are incorporated in Singapore;
 - (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 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;
 - (f) authorised benchmark administrators;
 - (g) authorised benchmark submitters;
 - (h) designated benchmark submitters; and
 - (i) the Depository,
- (each a “financial institution”).

[CMG-N02 (Amendment) 2014]

[CMG-N02 (Amendment) 2018]

Definitions

2 For the purpose of this Notice —

“critical system” in relation to a financial institution, means a system, the failure of which will cause significant disruption to the operations of the financial institution or materially impact the financial institution’s service to its customers, such as a system which —

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

“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;

“relevant incident” means a system malfunction or IT security incident, which has a severe and widespread impact on the financial institution’s operations or materially impacts the financial institution’s service to its customers;

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

“system malfunction” means a failure of any of the financial institution’s critical systems.

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

Technology Risk Management

4 A financial institution shall put in place a framework and process to identify critical systems.

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

6 A financial institution shall 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 financial institution shall 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 financial institution shall notify the Authority as soon as possible, but not later than 1 hour, upon the discovery of a relevant incident, other than a relevant incident arising from the circumstances set out in regulations ~~9(1)8(2)(a) and (b), and 23(1)(e)21(d)~~ of the Securities and Futures (Organised Markets) Regulations ~~2005~~2018 (“Markets Regulations”), regulation 9(1) of the Securities and Futures (Trade Repositories) Regulations 2013~~-, and~~ regulation 11(1) of the Securities and Futures (Clearing Facilities) Regulations 2013~~-, and~~ regulations 11(1)(e) and 19(2)(b) of the Securities and Futures (Financial Benchmarks) Regulations 2018 (“Financial Benchmarks Regulations”).

[CMG-N02 (Amendment) 2014]

[CMG-N02 (Amendment) 2018]

8 A financial institution shall, within 14 days or such longer period as the Authority may allow, from the discovery of the relevant incident as described in paragraph 7 or a relevant incident arising from the circumstances set out in regulation ~~23(1)(e)~~21(d) of the Markets Regulations, as the case may be, submit a root cause and impact analysis report to the Authority. The report shall 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 financial institution's —
 - i. compliance with laws and regulations applicable to the financial institution;
 - 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.

[CMG-N02 (Amendment) 2018]

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

Effective Date

10 This Notice shall take effect on 1 July 2014.

*Note on History of Amendments:

1. CMG-N02 (Amendment) 2014 with effect from 1 July 2014.

2. CMG-N02 (Amendment) 2018 with effect from 8 October 2018.