FREQUENTLY ASKED QUESTIONS

GUIDELINES ON TECHNOLOGY RISK MANAGAMENT

(Date of Issuance: 1 August 2023)

PART A: General

1. What is the objective for the issuance of the *Guidelines on Technology Risk Management* (Guidelines)?

The Guidelines are issued to promote technology risk management among capital market entities. The outcome desired by the SC for the Guidelines is two-pronged, that is for all capital market entities to have a robust and sound framework which promotes strong oversight and management of technology risks, and ultimately for the capital market to be cyber resilient.

2. When is the effective date of the Guidelines?

To allow all capital market entities sufficient time to familiarise themselves with the requirements of the Guidelines for purposes of compliance, the Guidelines are expected to come into force by the third quarter of 2024. The SC will make a public announcement on the effective date prior to the Guidelines coming into force.

3. Are capital market entities required to still comply with the Guidelines on Management of Cyber Risk after the issuance of the Guidelines?

Yes, the SC expects all capital market entities to continue complying with existing guidelines including the *Guidelines on Management of Cyber Risk* during the familiarisation period of the Guidelines (i.e. after issuance of the Guidelines, but before its effective date in 2024), while working towards putting in place effective controls, policies and procedures to ensure compliance with the Guidelines by the effective date.

Capital market entities are encouraged to comply with the requirements of the Guidelines as soon as possible.

4. Are capital market entities required to still comply with the requirements relating to outsourcing arrangements in other existing guidelines?

Yes, the SC expects all capital market entities to continue complying with all requirements relating to outsourcing arrangements in existing guidelines in addition to the requirements in the Guidelines.

5. Who are the Guidelines applicable to?

The Guidelines will apply to all capital market entities licensed, registered, approved, recognized or authorized by the SC as specified in the Guidelines. Please refer to definition of "capital market entities" in paragraph 4.01 of the Guidelines.

6. What is the consequence for breaching the Guidelines?

SC may take administrative actions against any person who breached the Guidelines under the securities laws administered by the SC once the Guidelines have come into effect.

7. For a capital market entity that is regulated by more than one regulatory body, which technology risk management requirements would apply?

Where a capital market entity is subject to more than one technology risk management-related requirements and there are differing requirements, the more stringent requirement shall apply. Please refer to paragraph 3.03 of the Guidelines.

8. My company is part of a group of companies which manages all technology risks within the group at the holding company level. What are the SC's expectations on my company vis-à-vis the requirements in the Guidelines?

If a capital market entity is operating and managed at a group level, the capital market entity may leverage on its group's technology risk framework, provided that such framework is sufficiently comprehensive and addresses areas specified in the Guidelines. Such arrangement is considered as an outsourcing arrangement under the Guidelines, thus the capital market entity and its board remain responsible for the outsourced functions.

9. Some of the requirements under the Guidelines may not be applicable to my entity. For example, we do not embark on cloud services. Does my entity still need to comply with the Guidelines?

A capital market entity is expected to comply with the requirements set out under the Guidelines. The extent and degree of application of the requirements is dependent on, amongst others, the type of capital market related services the capital market entity carries on and its level of technology dependency.

As such, capital market entities are expected to assess the application of the various requirements in the Guidelines and ensure that the extent and degree of implementation commensurate with their respective business operations as well as the level of technology risk exposures. If, for example, the capital market entity does not embark on cloud services, then it follows that the requirements pertaining to cloud services would not apply to the capital market entity.

PART B: Technology Risk Management Framework

10. Does a capital market entity have to appoint two individuals to independently take on the responsibilities under paragraph 5.02(h)(i) and paragraph 5.02(h)(ii) of the Guidelines?

A capital market entity may appoint one individual to take on both responsibilities under paragraph 5.02(h)(i) and paragraph 5.02(h)(ii) of the Guidelines. In this regard, the appointment of one or more individuals to take on the responsibilities envisaged under these provisions must be premised on assessment and determination by the capital market entity of the ability of the relevant individual(s) identified towards ensuring proper discharge of the role towards ensuring compliance of the Guidelines.

11. Pursuant to paragraph 7.04 of the Guidelines, a capital market entity must ensure there are adequate personnel, including key stakeholders to oversee and manage technology-related projects. Who are these key stakeholders and what involvement are expected from them?

The key stakeholders are the relevant personnels whose role or function, or area of work, may or will be impacted or affected by the technology-related project. Their involvement may include serving as project co-ordinator and advisor, or being responsible for deliverables, project costs and schedules, or providing feedback and input.

12. What suitable cryptographic controls may be implemented by my company to safeguard the confidentiality, authenticity and integrity of its sensitive data from unauthorised access and unintentional disclosure as required under paragraph 7.19 of the Guidelines?

Suitable cryptographic controls may include data encryption, digital signature or message authentication codes or cryptographic techniques, all of which may be used to obtain evidence of the occurrence or non-occurrence of an event or action (non-repudiation) and to verify users with the right access (authentication).

13. My company usually conducts testing exercises of our IT Disaster Recovery Plan (DRP) together with our business continuity plan (BCP) annually. Can we continue to do so or does the SC expect the IT DRP testing exercise to be conducted more than once a year to meet the requirement under paragraph 7.56 of the Guidelines?

The objective of conducting IT DRP is to ensure staff and relevant stakeholders are familiar with their roles, responsibilities, and actions that are expected to be performed when disaster recovery is activated and that measures put in place operate as planned during a disaster. As such, the frequency of the IT DRP should be determined based on the capital market entity's assessment of the criticality of its IT systems to its business and services with a view of achieving the said objective.

A capital market entity may continue to conduct its IT DRP testing exercise together with its BCP testing exercise on an annual basis provided that the objective mentioned is achieved. However, the capital market entity should consider increasing the frequency if needed.

14. Are capital market entities required to conduct due diligence on its existing service providers under paragraph 8.02 of the Guidelines?

Capital market entities are expected to conduct due diligence prior to onboarding new third-party service providers or prior to renewing contracts of existing service providers.

In addition, as the capital market entities are required to ensure that existing service providers are capable of fulfilling their functions and services, they are also expected to conduct periodic assessment under paragraph 8.04 of the Guidelines.

15. Pursuant to paragraph 9.26 of the Guidelines, who are the key stakeholders who should be involved in the cyber simulation exercise?

As part of a cyber simulation exercise, a capital market entity should consider the involvement of key stakeholders, including senior managers, employees, vendors, and dependent parties, such as business partners, who directly impact the capital market entity's ability to achieve its business objectives. By involving these stakeholders, the capital market entity can ensure a comprehensive understanding of potential cyber security risks and develop effective strategies to mitigate them.

16. Pursuant to paragraph 9.28 of the Guidelines, how should a capital market entity perform an adversarial attack exercise?

Adversarial attack exercise (or also known as red teaming) is conducted to identify the vulnerabilities and weaknesses in an entity's security defenses. In this exercise, cyber security professionals assume the role of an attacker with the aim to identify weaknesses in the system defenses by mimicking techniques, tactics and procedures (TTP) practiced by real world attackers. The exercise takes place within the entity's real operating environment, enabling them to simulate various breach and attack scenarios towards pinpointing shortcomings in their personnel, procedures, and technologies.

17. Pursuant to paragraph 10.01 of the Guidelines, when should a capital market entity notify the SC of any major technology-related services or major enhancement on its critical systems?

A capital market entity should notify the SC prior to implementing any major technology-related services or major enhancement on its critical systems. Typically, this would mean at a stage where the necessary testing has been conducted and prior to such services or enhancements are available for use or begin operating (i.e. prior to go-live date).

18. Pursuant to paragraph 1(b) of Appendix 3 of the Guidelines, a capital market entity should have a workforce capable of managing a broad set of stakeholders. Who are these stakeholders?

The stakeholders are people who may be affected or have an interest in the artificial intelligence (AI) and machine learning (ML) systems or the decisions made by the AI and ML systems, which include but is not limited to users and clients of the capital market entity.