FREQUENTLY ASKED QUESTIONS
GUIDELINES ON TECHNOLOGY RISK MANAGAMENT
(Date Issued: 1 August 2023)
(Date Revised: 19 August 2024)

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. Are the requirements in the Guidelines on Management of Cyber Risk still applicable on and after the coming into effect of the Guidelines?

No, as this is superseded by the Guidelines which are applicable to capital market entities.

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

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

4. To whom does the Guidelines apply to?

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

5. What is the consequence for breaching the Guidelines?

The 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.

6. 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.

7. Where an entity is applying for a Capital Markets Services License (CMSL) or is seeking to be registered, approved, recognised or authorised by the SC, when is such entity required to comply with the Guidelines?

The Guidelines are applicable on a capital market entity as specified in the Guidelines from the date on which such capital market entity obtains its CMSL or is registered, approved, recognised or authorised by the SC.

However, an applicant may also be required to demonstrate its compliance with the requirements of the Guidelines as part of the application process.

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 its group's technology risk framework, provided that such framework is sufficiently comprehensive and addresses areas specified in the Guidelines. Such an 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 such requirements?

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, among others, the type of capital market related services the capital market entity carries on and its level of technology dependency. Please refer to paragraph 2.02 of the Guidelines.

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 do 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. Does a capital market entity need to have a dedicated internal technology audit function, or can the function be outsourced to a third-party service provider?

The technology audit function can either be performed internally or outsourced to a third-party service provider so long as the function maintains its independence. In the case where a third-party service provider is appointed for the audit function, a capital market entity must comply with Chapter 8 of the Guidelines on technology service provider management.

12. 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.

13. 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 to safeguard the confidentiality, authenticity, and integrity of sensitive data may include data encryption, digital signature or message authentication codes or cryptographic techniques. These measures 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).

14. 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.

15. 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.

16. Assuming a capital market entity is a small company and does not depend heavily on sophisticated technology, would the capital market entity still be required to carry out cyber simulation exercise to comply with paragraph 9.26?

Yes, a capital market entity is required to conduct cyber simulation exercises even if its operations are not heavily reliant on sophisticated technology. In today's digitalisation era, elements like e-mail, laptops, and smartphones are essential for business operations and still pose cyber security risks to its operations, business and clients. As such, it is important for all capital market entities to engage in some form of cyber simulation exercise such as, at minimum, a tabletop exercise. The exercise should be tailored to a capital market entity’s own risk appetite.

17. 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.

18. Is the Capital Market Cyber Simulation (CMCS) organised by the SC adequate to fulfil the cyber simulation exercise requirements outlined in paragraph 9.26 of the Guidelines?

No, capital market entities must carry out their own cyber simulation exercises that commensurate with the risk appetite of the entity. The CMCS organised by the SC is aimed to improve cyber risk awareness and hygiene in the capital market and strengthen the cyber resilience of our capital market entities.

19. 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 a cyber attacker with the aim to identify weaknesses in the system defenses by mimicking techniques, tactics and procedures (TTP) practiced by real world cyber 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. A capital market entity should perform such adversarial attack exercise, where feasible.

20. 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).

21. What qualifies as "major technology-related services or enhancements" under paragraph 10.01 of the Guidelines?

In determining whether a technology-related service or enhancement it proposes to implement is "major" or otherwise, a capital market entity should consider the risk exposure and potential impact that the proposed technology-related service or enhancement may have on the capital market entity's business operations or clients.

22. What documents should be submitted as attachments with the notification form in Appendix 4?

The notification form in Appendix 4 for technology-related implementation should be submitted together with any supporting documents which is relevant and deemed necessary by the capital market entity (e.g. approval(s) from the relevant internal parties, details on the changes made, etc).

23. Are capital market entities required to report all technology incidents regardless of its severity under paragraph 10.03 of the Guidelines?

A capital market entity is required to immediately notify the SC upon detection of any technology incidents *that affects its business operations or clients*. If an entity is unsure if an incident has such effect, it is recommended for the capital market entity to report such incident to the SC.

24. Are capital market entities required to report all cyber incidents regardless of its severity under paragraph 10.03 of the Guidelines?

Yes, a capital market entity is required to immediately notify the SC upon detection of any cyber incidents, regardless of its severity.

25. What are examples of near miss events under paragraph 10.03 of the Guidelines?

Near miss events are events which have a high potential to be an incident but were detected and mitigated before any substantial impact occurred. There are two categories of near miss events as follows:

(i) Events which have a high potential to become *technology incidents* that may potentially affect its business operations or clients

An example would be the case where a capital market entity's primary Internet Service Provider (ISP) was down for a period of time which could have affected the capital market entity's business operations and clients, but this was pre-empted as the capital market entity was able to detect and mitigate the event by switching to their alternative ISP.

(ii) Events which have a high potential to become *cyber incidents*

Examples of events that are under this category include direct denial of service (DDoS) attempts, intrusion attempts, and unauthorised access attempts.

26. Are capital market entities required to comply with reporting requirements relating to technology incident or cyber incident in other relevant SC Guidelines if such capital market entities have submitted a report in accordance with the Guidelines?

No, capital market entities that have complied with the reporting requirement in the Guidelines will be deemed to have complied with the reporting requirements relating to technology incident or cyber incident in other relevant SC Guidelines.

For example, if an electronic application provider has submitted a report via the Vault on a cyber incident, the electronic application provider will not be required to submit another report on the same incident under the *Prospectus Guidelines*.

27. Can capital market entities edit or update their report in the Vault system after submission to the SC?

Yes, capital market entities may edit or update their report in the Vault system after submission. We strongly encourage capital market entities to first submit their reports to the SC upon detection of an incident or event in accordance with paragraph 10.03 of the Guidelines and thereafter, update their reports on the Vault system with the latest information upon conducting their investigation on the incident or event.

28. 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.