"Guideline on Cybersecurity" ("GL20")
Frequently Asked Questions

The Insurance Authority ("IA") issues these frequently asked questions ("FAQ") with the aim of providing further guidance to authorized insurers in respect of GL20.

This FAQ is not intended to be a comprehensive guide and does not constitute legal advice. Authorized insurers are advised to seek professional legal advice if they have any questions in relation to the application or interpretation of the relevant provisions of GL20.

This FAQ does not have the force of law and should not be interpreted in a way that would override the provision of any law. The IA reserves the right to review and update this FAQ from time to time. Unless otherwise specified, words and expressions in this FAQ shall have the same meanings as given to them in GL20.

Q1. Are any assessments under Cyber Resilience Assessment Framework ("CRAF") required to be carried out with respect to each new product launch by an authorized insurer to which CRAF is applicable?

A1. The inherent risk and cybersecurity maturity assessments under CRAF should be conducted at least every three years (see Chapter 1.2.3 of CRAF). They are not required to be carried out whenever a product launch is anticipated or after the product has been launched. However, an authorized insurer may conduct the assessments if a new product launch is expected to result in any major changes to its business nature or technologies (e.g. a new digital channel or technology would be used in the distribution of the new product, or new / additional systems of external organizations would be integrated to the insurer's system to provide services to their customers) so to assess whether its inherent risk rating would be materially affected by the new product launch and if so, whether its cybersecurity is robust enough to respond to the changes which might be brought by the sale of the new product or any related services to its customers.

Q2. It is stated in Chapter 1.2.3 (Frequency) of CRAF that an insurer should, upon the IA's request, conduct the assessments on an ad hoc basis when the IA considers it appropriate. Under what circumstances an authorized insurer would be requested to conduct assessments on an ad hoc basis? How would such assessments affect the three-year assessment cycle?

An authorized insurer (to which CRAF is applicable) would only be requested by the IA to conduct the assessments (or any part of them) in CRAF on an ad hoc basis under specific circumstances, for example, the IA has concern whether the assessment results submitted by the insurer reasonably reflect its inherent risk and cyber security resilience maturity, or a cyber attack occurred and the IA has concern about the robustness and effectiveness of the insurer's cybersecurity controls. In the event where ad hoc assessments are conducted and subject to the extent of the ad hoc assessments, the normal assessment cycle may re-commence 3 years after the completion of the ad hoc assessments unless otherwise directed by the IA.

Q3. Is there any requirement on the timing and reporting of completion of remediation actions for identified issues?

A3. According to the submission protocol stated in Chapter 1.2.6 of CRAF, all remedial actions should be completed in a timely manner but no later than the next assessments are due (typically performed every three years).

How long an authorized insurer should take to complete a remediation action will depend on the circumstances of each case. In general, an insurer should categorize, prioritize and complete a remedial action within a reasonable time to minimize cyber risk exposure. The authorized insurers should regularly communicate the progress of their remediation action plan to the IA, including an update on the status of each identified gap and actions taken to address them, and reasons for any delay (if applicable). The frequency of communication with the IA regarding remediation progress may vary depending on the numbers and severity of the identified issues and the remediation plan. In general, insurers should provide updates to the IA at least annually or on shorter timeframe as specified by the IA.

Q4. Regarding the indicator "Cloud computing services hosted externally to support critical activities" under Category 1 of the Inherent Risk Assessment Matrix in Annex A to CRAF, would the adoption of Software as a Service ("SaaS") be considered as public cloud usage?

A4. Yes, adoption of SaaS would be considered as public cloud usage. SaaS utilises the public cloud to provide services to customers and business data would be transmitted and/or stored in the public cloud. Authorized insurers which adopt SaaS do not have control over SasS. For example, the IT infrastructure of SaaS is not maintained by the insurers. Neither do they monitor the operation of SaaS on a regular basis. It should be noted that only cloud usage for supporting critical activities is within the scope of this indicator.

Q5. Who should be considered as "third party" for purpose of carry out third party risk assessment under Domain 7 of the cybersecurity maturity assessment?

A5. "Third parties" in Domain 7 refer to those parties with whom an authorized insurer has established external network connections. Some examples include:

- Cloud service providers which host the insurer's systems and data;
- Business partners such as insurance brokers, hospitals and clinics which store customer and transaction data of the insurer;
- Service providers engaged by the insurer to perform services which involve data processing, e.g. know-your-customer screening, claims administration and policy administration, etc.

In general, "third party" does not include:

- Non-IT vendors (e.g., physical security service company).
- IT vendors with whom the insurer do not have any direct connection established (e.g., off the shelf software providers).
- Governments, public utilities and financial market infrastructure ("FMI"), e.g., credit card issuers).

Q6. According to Chapter 1.2.5 (Sampling), sample-based testing of controls should cover samples taken from at least the preceding 6 months if the cyber resilience assessment is to be conducted for the first time, and samples from at least the preceding 12 months for any subsequent assessments." Can an authorized insurer use samples taken from a period earlier than the preceding 6 months for conducting its cyber resilience assessment for the first time?

A6. Yes, authorized insurers may use samples taken from a period earlier than the preceding 6 months for conducting its cyber resilience assessment for the first time. The IA recognizes that some insurers may need more time to put in place or improve their cybersecurity controls, of which samples will be taken for the purpose of their cyber resilience assessment for the first time. The 6-month sampling period is intended to provide those insurers with a reasonable timeframe to do so before the assessment is conducted. If, however, an insurer has already had cybersecurity controls in place for a longer period of time, e.g. 6 to12 months, an extended sampling period should be adopted.