

To: Secretary General Sergio Mujica
International Organization for Standardization
ISO Central Secretariat
Chemin de Blandonnet 8
CP 401
1214 Vernier, Geneva
Switzerland

Date: 15 March 2019

Subject: Global Federation of Insurance Associations comments on ISO/IEC 27102

Dear Secretary General Mujica,

The Global Federation of Insurance Associations (GFIA), which represents companies that account for 89% of total insurance premiums worldwide, wishes to express its concerns with the development process of proposed standard ISO/IEC 27102, which provides guidelines for cyber insurance. GFIA takes the view that it is premature to develop such standardising guidelines on cyber insurance at a time when markets are still developing.

In addition, GFIA is particularly concerned that ISO is developing guidelines about cyber insurance without sufficient and adequate involvement of the insurance industry. While GFIA understands that there are different models for consultation with stakeholders due to the unique structure of ISO as a membership organisation, in this situation, GFIA is of the view that direct outreach and interaction with insurers is warranted regardless of process. Involving the insurance sector directly would limit the risk of misunderstanding of how cyber insurance works in practice.

Cyber insurance is a valuable risk mitigation tool that serves as a useful component to a business's overall security programme. For this reason, GFIA would underline the following general comments about any initiatives aiming to standardise cyber insurance product features:

- The cyber insurance market is continually evolving to meet the changing threat landscape and consumer demands. Standardisation in this area will inevitably become quickly outdated and will not provide an accurate resource or guidance for businesses. This will only serve to frustrate rather than benefit the insurance consumer.
- Cyber insurance coverage, risk assessment procedures and information requests are often tailored to meet the needs of individual businesses. This is especially the case of large companies. On the other hand, the amount of information required from an SME will likely be considerably smaller. In addition, cyber insurance elements are tailored to sector-specific needs. For instance, the needs of the healthcare industry will differ from technology providers or the payment services sector. Therefore, a standard guideline will not meet everyone's needs.



GLOBAL FEDERATION OF INSURANCE ASSOCIATIONS

- Similarly, the cyber insurance market is still a developing market and, as such, insurance policies and terminology are developing organically in tune with consumer demands at a rapid rate. A generalised standard cannot address these important differences.

Finally, GFIA is not aware of another international standard applicable to a particular line of insurance business and does not agree with the development of one for cyber insurance in light of the comments made above.

ISO's education objective for standard ISO/IEC 27102 is commendable and there are positive aspects of the document. As such, GFIA would welcome the opportunity to present its views on cyber insurance and discuss its concerns with you further.

Kind regards,

A handwritten signature in black ink, appearing to read "St. A.", is positioned below the closing.

Steve Simchak

Chair of the GFIA Cyber Risks working group (steve.simchak@apci.org)

About GFIA

Through its 41 member associations and 1 observer association, the Global Federation of Insurance Associations (GFIA) represents the interests of insurers and reinsurers in 64 countries. These companies account for around 89% of total insurance premiums worldwide. GFIA is incorporated in Switzerland and its secretariat is based in Brussels.