GLOBAL FEDERATION OF INSURANCE ASSOCIATIONS

August 2022

General principles of effective supervision of insurers' operational resilience

1. The development of international regulatory standards and domestic approaches for operational resilience in the insurance sector must be risk- and principles-based in order to allow firms the flexibility to develop a framework that suits their own business model and operating model, and the risks of disruption they face.

Technological changes and the changing tactics of cyber criminals will make any rules-based regulatory systems rapidly obsolete. To the greatest extent possible, supervisors should adopt an own risk management approach for supervised insurers in which — taking a similar approach to an Own Risk Solvency Assessment (ORSA) — an insurance group undertakes an internal process to assess the adequacy of its risk management and its current and prospective positions under different stress scenarios. Furthermore, recognising that third-party service providers (TPSPs) encompass an enormous range of different types of services, supervisors must not assume that supervisory approaches that are appropriate for one type of third-party service are also appropriate for others.

2. Supervisory approaches intended to address operational resilience in the insurance sector must reflect the insurance sector, and not adopt inappropriate systemic risk frameworks from the supervision of other financial sectors.

Insurance supervisors sometimes borrow the concept of "critical" business services or functions from the banking context and apply it to insurers, where "critical" refers to the risk that a disruption to a firm's business service(s) or function(s) poses a systemic risk to a jurisdiction's financial system or economy. While systemic risks are apparent in the banking sector, given their role in the payment and settlement system or custodial services, a potential disruption of business services and functions from the insurance sector would not jeopardise financial stability or the economy. As a result, GFIA believes it is inappropriate to borrow such bank-centric systemic risk concepts for use in insurance operational resilience supervision. Insurers should be subject to one, exclusive set of data security rules and there should only be one supervisor responsible for data security in any jurisdiction.

3. When supervising internationally active insurance groups that operate in multiple jurisdictions, operational resilience rules should be consistent and permit global, group-wide operational resilience practices.

Group-wide approaches to resilience allow insurers to rationalise the number of systems to be monitored and maintained, provide additional options to mitigate physical risks and create the ability to leverage global teams

Global Federation of Insurance Associations (GFIA)
Secretariat: rue du Champ de Mars 23, 1050 Brussels, Belgium
Tel: +32 2 894 30 81 E-mail: secretariat@GFIAinsurance.org
www.GFIAinsurance.org

and services for continuous, real-time monitoring and response. Supervisors should support and facilitate the use of such group-wide practices. Supervisors should also be consistent in the use of operational resilience concepts and terminology across jurisdictions and authorities. Fragmented terminology, rules and guidance in different jurisdictions make it more difficult for supervisors to coordinate, weaken group-wide operational resilience efforts, create uncertainty that impedes innovation and ultimately impose a significant cost and compliance burden on the industry.

4. Supervisory approaches to operational resilience must take proper account of the benefits that TPSPs offer in addressing supervisory concerns around TPSPs, particularly with regard to cloud service providers (CSPs).

CSPs often use the latest technology and practices to protect clients in the face of cyber threats and cyber-event mitigation and response. Having a resilient business model capable of efficiently responding to and recovering from a cyber disruption is vitally important. CSPs can also contribute to a client's resilience by giving the client the ability to move data from one location to another or store data in multiple locations simultaneously. An individual insurer could not replicate these CSP benefits and ongoing upgrades in a cost-efficient manner.

5. Audits of TPSPs, when required, must be reasonable and proportionate.

CSPs and other TPSPs may be subject to dozens of internal and external audits on the same or similar topics, conducted on behalf of different clients, in addition to the self-certification or third-party certifications that CSPs themselves may undertake. The vast array of duplicative, uncoordinated audits can be onerous and reduce the efficiency or technological developments of a TPSP.

Contacts

Steve Simchak, chair, GFIA Cyber Risks Working Group (steve.simchak@apci.org)

Pierre Lebard, GFIA secretariat (secretariat@gfiainsurance.org)

About GFIA

The Global Federation of Insurance Associations (GFIA), established in October 2012, represents through its 40 member associations and 1 observer associations the interests of insurers and reinsurers in 67 countries. These companies account for 89% of total insurance premiums worldwide, amounting to more than $4 trillion. GFIA is incorporated in Switzerland and its secretariat is based in Brussels.