GLOBAL FEDERATION OF INSURANCE ASSOCIATIONS

18 December 2024

GFIA response to Financial Stability Board (FSB) consultation on Format for Incident Reporting Exchange (FIRE)

General

1. Please provide any general comments to the FIRE design. Please elaborate on the preconditions (for instance, extent of uptake by individual authorities, extent of convergence) you deem necessary in order for FIRE to be successful.

The Global Federation of Insurance Associations (GFIA) and its members are pleased to respond to the Financial Stability Board (FSB) Format for Incident Reporting Exchange (FIRE) Consultation Report. GFIA recognises and appreciates the FSB's long-standing leadership in addressing market fragmentation and encouraging coordination, consistency and cooperation among member jurisdictions, and with other global standard-setting bodies.

GFIA also commends the FSB for its critical work in promoting greater harmonisation around cyber security and cyber risk practices, including in this case regarding incident reporting across financial institutions and reporting authorities around the world.

In general, GFIA supports the FSB's FIRE proposal. If the whole global financial sector and all supervisors would agree to a common framework for reporting, this would actually make the job of global organisations much easier; however, some regulators are already steps ahead and have defined their own reporting format and processes. GFIA expects that, in the future, international jurisdictions with more discretion and subjective standards, such as the NYDFS, and the EU, with more objective standards that cause a high level of reporting, will converge. If FIRE can help facilitate this process, it is welcome. Until that convergence takes place, it would be in the best interests of entities operating under many different global regulatory schemes to have a more subjective standard, as opposed to the more rigid objective standards.

Consistency of reporting would also be helpful. GFIA would recommend that the FIRE effort be directed at defining the minimum necessary information needed by the regulatory bodies as a universal standard. Common terms or taxonomy will help, but the effort must be directed at defining what information regulatory bodies need.

As in previous comments of this nature, GFIA would ask that the FSB consider the additional strain posed by conflicting compliance requirements, particularly where local laws require the preservation of confidentiality and prohibit information sharing, while other supervisory groups request or require that information to be shared.
GFIA also encourages proportionality and respect for confidentiality. Once those conditions are met, there are better opportunities for sharing information without potential unintended consequences, compliance burden or legal repercussions.

GFIA supports the Testing Phase that, as described in the consultation, is apparently underway to validate the design and robustness of FIRE using different incident types and scenarios. GFIA also endorses the proposed workshop planned for 2027 to review experiences and determine the need for revisions after the next version of FIRE is published. Additionally, GFIA encourages ongoing consultation with impacted stakeholders.

Case study - FIRE from a Canadian context

In Canada, the Office of the Superintendent of Financial Institutions (OSFI) defines, in its Technology and Cyber Security Incident Reporting Advisory, criteria for a "reportable incident" and the requirement to report within 24 hours, or sooner if possible.

In addition, OSFI has their own "OSFI Technology and Cyber Incident Report" that needs to be completed, including subsequent reporting requirements based on the severity, impact and velocity of the incident which determine the method and frequency of updates.

The province of Quebec's *Autorité des marchés financiers* (AMF) Regulation Respecting the Management and Reporting of Information Security Incidents defines an "information security incident" and the requirement to report an incident within 24 hours. The AMF requires their form to be filed via their website, with subsequent reporting requirements including updates no

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

later than three days after the initial notice is given and no later than every three days thereafter, until a notice is sent confirming that the incident is under control.

The above highlights the regulatory incident reporting requirements in Canada for OSFI and the AMF. These regulators have their own technology and cyber incident definitions, reporting formats, tools to use for filing reports, and subsequent reporting requirements. How will the FIRE approach achieve harmonisation given these varying differences? Currently, the FIRE approach does not define common reporting triggers, deadlines or mitigation approaches and expects that "Authorities could decide the extent to which they wish to adopt FIRE, if at all, based on their individual circumstances". How will this be done? The Canadian regulators need to make decisions here and the federally-regulated financial institutions (FRFIs) would comply as instructed.

Furthermore, 99 information items are defined, 51 are optional, and 48 are required, "allowing Authorities to decide which to implement based on their needs". If the premise of the FIRE approach is to harmonise and not create computing operational challenges, this appears overly complex given the existing simplified reporting forms available by the Canadian regulators (eg approximately 15 data fields). The number of data points required should be revisited. Resources will be focused on containing the breach and should not be burdened with onerous reporting.

Lastly, to achieve full alignment with FIRE, implementing jurisdictions must include all essential information items, meet baseline optionality requirements, use compatible field types, and adhere to enumerated lists. Partial implementation may still offer some coherence. It is unclear if the FIRE approach will produce added benefits. While a converged approach to reporting is welcomed, it does not align with the existing reporting templates required by the Canadian regulators.

2. Please give examples of the various ways in which FIRE can be used in your company's incident reporting, and/or of use cases of FIRE, and whether the design adequately facilitates these use cases.

There are three distinct reporting types that are part of the FIRE approach: (1) institution-initiated reporting, (2) authority-initiated reporting, and (3) periodic reporting.

- (1) **Institution-initiated reporting:** Internally, many organisations have their own tools and processes for reporting and tracking operational and cyber related risks. These tools may be mandated internally and required for group-wide reporting. Processes already in place facilitate and consolidate reporting across international organisations, for example, and ensure consistent and comparative reporting among various units. It may not always be possible to deviate from internal and organisational-wide methods. In international organisations, local decisions most often are made considering the global requirements.

- (2) **Authority-initiated reporting:** If the Canadian regulators decide to use the FIRE approach and eliminate their own unique reporting requirement/ tools we would use for external reporting requirements.

Scope of FIRE

3. Is the FIRE design appropriately scoped? (Choose: Not at all, Slightly, Moderately, Mostly, Completely)

Not at all. These definitions would have to be aligned with domestic regulators based on their respective guidelines.

4. In addition to the primary scope covering incident reporting by financial institutions to their regulators, does the FIRE design appropriately facilitate its use for reporting of third-party service providers? (Choose: Not at all, Slightly, Moderately, Mostly, Completely)

Not at all. In Canada for example, some organisations are required to use a third party risk management (TPRM) tool mandated by their parent company. The requirements stemming from the OSFI TPRM Guideline would need to be aligned with the FIRE design for reporting purposes.

GLOBAL FEDERATION OF INSURANCE ASSOCIATIONS

Specific questions and technical questions

5. For each of the FIRE pillars, is the design appropriate? Please consider: (a) number and nature of information elements, (b) their requested and permissible content, and (c) their relevance for the different reporting phases in the lifecycle of an incident.

(i) Reporting details (section 1.1 of the Design)

Slightly. Design is sufficient in terms of contact details and is permissible for content reporting purposes.

(ii) Incident details (section 1.2 of the Design)

Not at all. Portions of the form cannot be filled out within 24 hours as the FRFIs will not have all the available information while the investigation is still taking place. Resource efforts will be focused on containing the actual breach and it becomes onerous when there are 48 compulsory data fields. PII should not be listed in the incident details – this should be explicitly noted.

(iii) Impact assessment (section 1.3 of the Design)

Not at all. How will international severity levels be harmonised? What is considered a Severity 2? Some organisations define severity impacts based on internal group-wide definitions mandated by their parent company, for instance, in order to handle global cyber incidents impacting various international units. How will severity levels be matched up between organisations and separately ones defined by the regulators?

(iv) Incident closure (section 1.4 of the Design)

Slightly. Design is sufficient as the data fields (eg causes identified, cause type, origin, lessons learned, etc.) are already required in existing reports by the Canadian regulators.

6. Please provide any comments on the data model and/or the XBRL taxonomy that are part of the consultation package.

The data model (DPM[5] method) / XBRL taxonomy as part of the package would require coordination with the Canadian regulators as these machine-readable versions of FIRE would need approvals with various systems.

Separately, organisations would need to align as well – organisations would need to coordinate with their parent company's requirements, which includes pre-determined formatting that does not currently support adopting the FIRE format. This would extend to all entitles within the international organisation as they would need to adopt for the use case to be justified and approved. Essentially, the data model/ XBRL taxonomy has to be flexible enough to create interoperability.

Contacts

Robert Gordon, chair of the GFIA Cyber Risks Working Group (robert.gordon@apci.org)

Marianne Willaert, GFIA secretariat (secretariat@gfiainsurance.org)

About GFIA

The Global Federation of Insurance Associations (GFIA), established in October 2012, represents through its 42 member associations and 3 observer associations the interests of insurers and reinsurers in 68 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.