The Asset Management Industry
SERVING INDIVIDUAL INVESTORS
INVESTMENT COMPANY INSTITUTE

MEMO# 35917

November 5, 2024

FSB Consultation on Format for Incident Reporting Exchange

[35917]

November 05, 2024

TO: ICI Members
ICI Global Members
Asia Regulatory and Policy Committee
Business Continuity Planning Committee
Chief Information Security Officer Committee
Europe Regulatory and Policy Committee
Global Information Security Officer Committee - London
Global Information Security Officer Committee - Tokyo
Global Operations Advisory Committee
Global Operations Advisory Committee - Asia
Operations Committee
Securities Operations Advisory Committee SUBJECTS: Cybersecurity
International/Global
Operations
Recordkeeping
Technology & Business Continuity RE: FSB Consultation on Format for Incident Reporting Exchange

On 17 October, the Financial Stability Board (FSB) published a consultation report on a Format for Incident Reporting Exchange (FIRE).[1] Responses to the Consultation are requested by 19 December 2024 and ICI plans to submit a response.

Overview

The Consultation sets forth a proposed template for incident reporting that is intended to support greater harmonisation of regulatory reporting of operational incidents by financial institutions. FIRE extends from the FSB's prior work on cyber resilience and the FSB notes that many authorities do not differentiate cyber incident reporting from broader operational incident reporting. In addition, the FSB suggests that financial institutions may choose to use FIRE in relationships with third-party service providers.

The FSB designed FIRE to support flexible implementation by authorities. To reach the goals of interoperability and harmonisation, the FSB is encouraging broad implementation of the

48 "essential" information items while acknowledging that authorities have flexibility to adopt these items. The remaining 51 items are optional, but their implementation would further promote the FSB's goals.

The Consultation does not include common definitions of reporting triggers, deadlines, or mitigation approaches.[2] This design choice is intended to maximise FIRE's flexibility and interoperability.

FIRE is designed with a common reporting method (Data Point Model (DPM), allowing for machine-readability, such as through eXtensible Business Reporting Language (XBRL)). Language of information items may be customised to support local language needs or pre-existing terminology within a jurisdiction. There are also several information items that use short or long text fields. Authorities may include supplemental guidance on the nature of descriptive information they wish to receive through these fields.

The FSB notes that there are two challenges to early assessments and reporting. In early stages, there may be low information confidence and the priority for the reporting entity needs to be focused on responding to the incident. Parties may also have limited awareness of impacts at the initial stage. Accordingly, the FSB designed the template so that reporting burdens are minimal at the outset of an incident.

Definitions to Support FIRE

Most of the definitions and terms used in FIRE can be found in the FSB's Cyber Lexicon,[3] but three new terms are included in the Consultation to extend to operational events:

Operational: Relating to people, processes, information, information systems, facilities, or external dependencies used to deliver one or more activities, functions or services.

Operational event: Any observable occurrence or change of a particular set of circumstances within the operational domain. Operational events sometimes provide indication that an operational incident is occurring.

Operational incident: An operational event that has been determined to have an adverse impact on an entity prompting the need for response and recovery.[4]

Summary of FIRE Information Items

The information items included in FIRE fall into four categories:

(1) reporting details,

(2) incident details,

(3) impact assessment, and

(4) incident closure.[5]

The reporting details address the reporting entity, the receiving entity, and contact details. To support interoperability across jurisdictions, entity identifiers for the reporting entity and their ultimate parent may include LEI codes, but these are not required. A field for local identifiers used within a jurisdiction is also included. Multiple recipient identifiers may be used, to facilitate simultaneous reporting to multiple entities. History and onward forwarding are also trackable.

Incident details include unique identifiers for the incident and related incidents; the nature and circumstances, which are refined as the incident evolves; actions taken or reactions since the prior report; and timing for key milestones. The reporting takes place over three stages (initial, intermediate, and final) and also indicates whether an incident is open, resolved, or closed. The covered incident types include (1) business disruption, system or execution failure; (2) compromise (non-disruptive); (3) data breach; (4) financial theft / fraud; and (5) information disorder.[6] While the Consultation does not define reporting triggers, the template provides a broad enumerated list of potential triggers.[7] The incident response fields include actions taken, actions planned, public reaction, communications issued, and bodies notified.

The impact assessment fields address severity, affected parties,[8] services and resources, and category of impact. The template includes two measures of severity, a standardised severity rating and the entity's internal severity rating.[9] The fields provide for assessments of the severity of financial, operational, reputational, legal/regulatory, and external impacts using these scales.[10] Geographic impact is also assessed. Service impacts focus on "how external parties interact with the reporting entity, rather than affected operations within the reporting entity"[11] while impacts to resources are assessed in terms of the disruption of the services that they support.[12]

The incident closure items describe the cause,[13] lessons identified and remedial activity, and supplemental documentation.

Next Steps

In parallel to the Consultation, the FSB is testing FIRE with industry stakeholders and will use feedback from testing and from the Consultation to finalise the FIRE template in mid-2025.

Approximately two years after implementation, the FSB plans to hold a workshop to determine whether any revisions are necessary.

Kirsten Robbins
Associate Chief Counsel, ICI Global

Notes

[1] FSB, Format for Incident Reporting Exchange (FIRE): Consultation report (17 October 2024) (the Consultation).

[2] Annex A describes the standardised field templates included in FIRE.

[3] FSB, Cyber Lexicon: Updated in 2023 (13 April 2023).

[4] Consultation at 3-4.

[5] Annex B of the Consultation provides an overview of all FIRE reporting fields and describes the optionality for different reporting phases.

[6] See Consultation at Annex C.

[7] See id. at 24.

[8] See id. at 30-31 for a list of descriptors for affected parties.

[9] See id. at 29-30.

[10] See id. at 38-41. Annex E provides a visual chart of the standardised severity scale and Annexes J to N illustrate the application of the standardised scale to financial, operational, reputational, legal / regulatory, and external impacts.

[11] Consultation at 32-33. Annex F describes the service disruption types.

[12] See Consultation at 36-37. Annex H provides a list of resource types with descriptions and examples and Annex I describes resource properties.

[13] See Consultation at 41-44. Annex O describes cause types.
