Format for Incident Reporting Exchange (FIRE): Consultation report

Response to Consultation

Investment Company Institute

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 Investment Company Institute (ICI) [1] appreciates the opportunity to comment on the Financial Stability Board's (FSB) consultation on a Format for Incident Reporting Exchange (FIRE) (the Consultation). [2] The importance of, and necessity for, effective information security increases with each passing day as bad actors remain intent on penetrating systems of financial institutions to access or exfiltrate their data. ICI's members have long taken seriously their obligation to protect their systems and the confidentiality of their non-public information against any type of threat – including cybersecurity threats. This is not surprising as our members' brands and success as a business are highly dependent upon investor confidence. Cybersecurity attacks or incidents could easily and quickly erode or destroy such confidence.

   We generally support the overall goal of the Consultation to facilitate greater harmonisation of regulatory incident reporting. A global asset management firm has many reporting requirements across all the jurisdictions in which it operates. Authorities' need for this information is critical, but the fragmented nature of these frameworks poses a significant challenge to firms with global operations. Although authorities share the goal of improving resilience through their individual reporting frameworks, resilience can degrade as firms spend critical resources to comply with divergent requirements.

   We agree that FIRE, a common reporting template with commonly defined information elements, can help firms identify similar requirements across regulatory frameworks and reduce duplicative reporting burdens, thereby supporting firms' ability to focus on the incident response. The flexibility of and limitations on the scope of FIRE's design, however, could limit its harmonising impact. Many of the challenges associated with divergent regulatory frameworks could remain.

   The FSB seeks to maximise authorities' flexibility to implement and customise the template, with more than half the information elements designated as optional. We agree that such

optionality is necessary to assure that implementation is consistent with an authority's mandate and its relevant regulatory framework. We encourage the FSB to ensure that FIRE could be fully implemented in conjunction with existing and forthcoming reporting requirements such as those issued under the Digital Operational Resilience Act (DORA), [3] the Network and Information Security Directive (NIS2), [4] the Critical Entities Resilience Directive (CER), [5] the Cyber Incident Reporting for Critical Infrastructure Act Infrastructure Security Act (CIRCIA), [6] and the United States Securities and Exchange Commission's (SEC) cybersecurity rules. [7] FIRE's flexible design may also promote wider partial implementation.

FIRE could reduce but would not eliminate the burden of preparing multiple reports. Despite convergence of certain reporting fields, global firms still could be required to make multiple filings (i) for jurisdictions that partially adopt FIRE and customise FIRE to their existing reporting framework and (ii) to accommodate different triggers, deadlines, and requirements for mitigating approaches and other aspects of incident response and recovery that FIRE does not cover.

We appreciate that FIRE's design promotes many of the FSB's Recommendations to Achieve Greater Convergency in Cyber Incident Reporting, [8] such as common data requirements and reporting formats (Recommendation 3) and phased and incremental reporting (Recommendation 4). Nevertheless, FIRE does not address other key aspects of divergent regulatory reporting requirements such as the need to protect sensitive information (Recommendation 16). We encourage the FSB to revise FIRE to include measures to address the sensitivity of reported information, considering, for example minimum cybersecurity standards for authorities receiving reported information. [9]

We also encourage the FSB to undertake further work to facilitate regulatory convergence and address 2023 recommendations that are outside of FIRE's scope.

Finally, while we appreciate the FSB's plan to review FIRE implementation and consider further refinements to enhance its effectiveness, conducting that exercise two years after the FSB finalises FIRE may not provide sufficient time to understand implementation challenges after authorities make any necessary regulatory changes to implement FIRE.

[1] The Investment Company Institute (ICI) is the leading association representing the global asset management industry in service of individual investors. ICI members are located in Europe, North America and Asia and manage fund assets of $47.1 trillion, including UCITS, mutual funds, exchange-traded funds (ETFs), closed-end funds, unit investment trusts (UITs) and similar funds in these different jurisdictions. ICI has offices in Brussels, London, and Washington, DC.

[2] FSB, Format for Incident Reporting Exchange (FIRE): Consultation Report (17 October 2024).

[3] Directive (EU) 2022/2554 (27 December 2022). See also Commission Delegated Regulation (EU) 2024/1774 (13 March 2024); Commission Delegated Regulation (EU) 2024/1772 (13 March 2024; Commission Implementing Regulation 2024/2956 (29 November 2024); Commission Implementing Regulation (EU) 2024/2956 (29 November 2024).

[4] Directive 2022/2555 (14 December 2022). See also Commission Implementing Regulation (EU) 2024/2690 (17 October 2024).

[5] Directive (EU) 2022/2557 (14 December 2022).

[6] 6 U.S.C. 681-681g (23 December 2022). See also Notice of Proposed Rulemaking, 89 FR 23644 (4 April 2024).

[7] 88 FR 51896 (4 August 2023).

[8] FSB, Recommendations to Achieve Greater Convergence in Cyber Incident Reporting (13 April 2023).

[9] In the United States, the Federal Information Security Modernization Act requires agencies to undergo an annual independent evaluation of their information security programs and practices.

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.**

Scope of FIRE

3. **Is the FIRE design appropriately scoped? *(Choose: Not at all, Slightly, Moderately, Mostly, Completely).* Please elaborate. Which, if any, amendments to the definitions of 'operational', 'operational event', and 'operational incident' as used in FIRE, would be needed.**

Moderately

We have supported FIRE in the context of cyber incident reporting to address some of the inherent practical and administrative challenges for global firms. [1] However, we have concerns regarding FIRE's expanded scope that broadly covers operational incident reporting. The justification for the expanded scope is that many authorities do not differentiate their approach to cyber incident reporting from their approach to operational incident reporting. [2] We recognise that authorities have recently focused on implementing new and amended cyber incident reporting frameworks (e.g., DORA, NIS2, CIRCIA Reporting Requirements, and the SEC cybersecurity rules), but we do not find that these approaches are consistently aligned with approaches to operational incident reporting. Indeed, in the EU, although the recently implemented DORA presents an EU-wide framework for cybersecurity, other cyber and operational incident reporting frameworks under NIS2 and CER involve implementation variation at the member state level and do not apply consistently to all financial institutions. Thus, operational incident reporting in remains fragmented and subsector specific.

Given the differences in reporting frameworks and the breadth of the new definitions (operational, operational event, and operational incident), we recommend that the FSB undertake additional study as to whether FIRE can effectively be used outside of the cyber incident reporting context. To be clear, we do not suggest that FIRE's finalisation and use

for cyber incident reporting should be delayed. Rather, we make this recommendation so that FIRE's impact on harmonisation and regulatory convergence for cyber incident reporting is not diminished because of the expanded scope.

[1] See Letter from Michael N. Pedroni to Secretariat to the Financial Stability Board re: FSB Consultative Document on Achieving Greater Convergence in Cyber Incident Reporting (22 December 2022), available at https://www.ici.org/system/files/2022-12/22-ici-cl-fsb-cyber-incident-reporting.pdf.

[2] Consultation at 3.

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 incidents to the financial institution by third-party service providers? *(Choose: Not at all, Slightly, Moderately, Mostly, Completely)*. Please elaborate. Which, if any, amendments to the current design would be helpful to fully cover this use case?**

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)

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

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

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

   For each FIRE pillar and each of subquestions (a) to (c), choose: Not at all, Slightly, Moderately, Mostly, Completely. Please provide comments in the related comment box for each FIRE pillar.

	(a)	(b)	(c)	Comment
(i)				
(ii)				
(iii)				
(iv)				

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