13 April 2023

Achieving Greater Convergence in Cyber Incident Reporting

Overview of responses to the consultation

On 17 October 2022, the Financial Stability Board (FSB) published a consultative document on achieving greater convergence in cyber incident reporting (CIR).[1] The consultative document:

- Sets out recommendations to address impediments to achieving greater convergence in CIR with a view to promote better practices;
- Advances work in developing common terminologies around cyber by proposing updates to the FSB's Cyber Lexicon; and
- Proposes the development of a format for incident reporting exchange (FIRE) to promote convergence, address operational challenges arising from financial institutions (FIs) needing to report to multiple authorities and foster better communication.

The FSB received 22 written responses from a variety of stakeholders.[2] The FSB also organised a workshop on 17 November 2022 and on 8 February 2023 to gather further feedback on the consultative document. This document summarises the comments raised in the public consultation and sets out the main changes made to the final deliverables in order to address them.

In general, there was broad support for the consultative document and the FSB's work to achieve greater convergence in CIR. Many respondents agreed with the six categories of practical challenges to achieving greater convergence identified in the consultative paper and offered additional evidence/case studies from their institutions to corroborate the FSB's findings in this regard. As such, the revisions to this section were largely editorial.

There were a number of points raised that translated to revisions to some of the recommendations to achieve greater convergence in CIR and to terms in the Cyber Lexicon. The concept of a format for incident reporting exchange (FIRE) also received strong support. Respondents emphasised the need to align with parallel activities (e.g. DORA) and suggested a broad list of stakeholders to consider as part of FIRE engagement.

---

1 FSB (2022), *Achieving Greater Convergence in Cyber Incident Reporting: Consultative Document*, October.

2 Non-confidential responses are available on the FSB website.

1. Recommendations to achieve greater convergence in CIR

A variety of feedback was received on the recommendations to achieve greater convergence in CIR. The majority of points were also discussed at the November workshop. Some of the more prevalent issues include:

- **Design of approach to CIR**. Some desire for the FSB to converge around one model for CIR, and be more prescriptive in terms of the reporting triggers, and how the phased reporting process should operate. Some expressed preference towards the use of materiality-based thresholds over reporting triggers that are simply based on incident discovery or occurrence, while there were also some who commented on the difficulty of using materiality-based thresholds as reporting triggers. Certain respondents also suggested that there may be a need to delineate between the process of 'incident notification' and 'reporting', raising the question of whether a 'notification' is separate from the reporting process or can be considered as the 'initial reporting'. One respondent also suggested that the FSB should standardise the triggers and information reported for each phase of the initial, intermediate and final reporting process. Some feedback was also received on the importance of incorporating proportionality within the design of CIR frameworks, and for authorities to ensure that the types of information collected through the CIR process are aligned with its objectives for CIR. Finally, there were also multiple comments that indicated a need for the FSB to further clarify the scope of incidents that would be reportable under Recommendation 8.

- **Scope and coverage.** Some respondents suggested for the FSB CIR recommendations to be extended to non-financial sector authorities, such as cyber security and data privacy authorities, to achieve even greater convergence and harmonisation in CIR.

- **Information sharing**. There was a common theme related to bi-directional information sharing, and specifically for authorities to provide a feedback loop to the industry on incidents reported and to foster greater information-sharing. There were varied suggestions for how this could be done, ranging from general commitments to share early warning indicators to more ambitious ideas, such as to develop a common information portal / notification hub and for authorities to report back to financial institutions if they experience a cyber incident themselves. There were also a few suggestions for the FSB to guide authorities to handle and process CIR information received according to certain principles or best practices, such as to anonymise data, restrict further sharing unless the FI in question is notified, and arrangements related to data security. Respondents opined that these would help augment trust in information sharing and reporting.

- **Trust**. Another common theme stemming from 'trust building' was support for 'safe harbour' provisions and 'liability protections' for financial institutions, with the general premise being that information shared by FIs should not be usable for legal action or proceedings, and that FIs should not be penalised or subject to greater supervisory scrutiny for sharing information relating to incidents.

- **Reporting channels**: A few respondents highlighted the importance of establishing 'back-up' channels to cater for situations where the primary ones may be inaccessible.

1.1. Changes to the recommendations

To address comments raised, a number of recommendations were revised. The most noteworthy changes include:

- **Recommendation 1: Establish and maintain objectives for CIR**. The recommendation was revised to include the concept of 'proportionality', and to add greater emphasis on the need for the incident information sought to align with financial authorities' CIR objectives and for financial authorities to engage with FIs to clarify their CIR objectives.

- **Recommendation 8: Promote timely reporting under materiality-based triggers.** The recommendation clarifies that 'near misses' are excluded and that the recommendation aims to promote timely reporting under materiality-based triggers. It also introduces the concept of allowing FIs to downgrade a reported incident, where warranted.

- **Recommendation 15: Pool knowledge to identify related cyber events and cyber incidents.** This recommendation now notes the benefits of financial authorities providing a feedback loop to FIs to enhance cyber resilience across the financial sector. To facilitate the building of trust, it also encourages financial authorities to take a constructive, rather than punitive, approach in the treatment of information shared by FIs, and to consider ways to foster bilateral information-sharing between financial authorities and FIs, as a complement to CIR.

- **Recommendation 16: Protect sensitive information.** The recommendation includes the need for financial authorities to consider establishing back-up communication channels to cover situations where the primary channel becomes unavailable to the reporting institutions.

While attempts were made to incorporate most of the remaining suggestions into the CIR recommendations, a small handful were ultimately not reflected in the revised recommendations after considering factors including: (i) the FSB's scope of work and mandate are focused on the financial sector, and (ii) there is general consensus that a 'one-size-fits-all' approach to CIR is not feasible given different authorities have varying objectives and mandates in relation to CIR.

2. Common terminologies for CIR

Responses largely lauded the FSB's efforts to revise the lexicon and emphasised the need for a common adoption of the terms to push consistency within the financial sector and to achieve greater convergence in CIR.

However, some points were raised for consideration, seeking further clarity on the proposed revisions for the terms.

2.1. Promote adoption, alignment and update of the lexicon

- **Align lexicon nationally and internationally.** Commenters noted that lexicon terms should be aligned with legislation and regulations at national and international levels, to avoid regulatory burden caused by duplication and overlapping of rules.
- **Promote adoption by public authorities.** According to respondents, the FSB should continue to promote the common adoption of the lexicon by public authorities. Two respondents stated that this would help the industry to integrate the definitions into their CIR practices, as currently they are bound to the definitions in the applicable legislation. One commenter suggested to introduce awareness-raising campaigns or other mechanisms to encourage the adoption and use of the Cyber Lexicon, which would support commonality in CIR reporting practices across jurisdictions and sectors, including authorities and supporting agencies.
- **Align lexicon with industry standards.** Three respondents noted that the lexicon would benefit from alignment with common industry standards (e.g. ISO, NIST for US-based companies), which are in most cases already integrated in internal processes. According to one respondent, the adoption of a coherent lexicon would ease implementation, as many organisations already embrace these definitions internally.
- **Lexicon updates**. It was stressed that the lexicon should be subject to regular updates in line with the evolving landscape.

2.2. Additional terms proposed

Respondents advanced numerous suggestions with respect to terms to add to the lexicon. After applying the criteria used in the development of the Cyber Lexicon in 2018, two terms were included, 15 terms were not included and five terms were deferred to the FSB group working on enhancing risks associated with third-party services (see Table 1).

Table 1: Additional Terms Proposed

Not included*	Deferred to TPR	Included
1. Authentication	1. Outsourcing	1. Cyber Attack
2. Authorisation	2. Supply Chain Risk	2. Zero-day Vulnerability
3. Blue, White and Purple Teaming	3. Third Party Risk	
4. Computer-security Incident	4. Third Party Service Provider	
5. Cloud Services	5. Third Party	
6. Cyber Impact Assessment		
7. Cyber Security Incident		
8. Encryption		
9. Materiality Threshold		
10. Major Cyber Incident		
11. Non-motive-based Operational Incident		
12. Operational Incident		
13. Significant Impact		
14. Trusted Entity		
15. Taxonomy to classify incidents		

2.3. Clarification of existing and newly proposed terms

Respondents also proposed clarifications and further edits for the definitions of 12 of the existing and proposed new terms (see Table 2).

Table 2: Proposed clarification of existing and new definitions*

No revision	Revised
1. Compromise	1. Cyber Alert
2. Cyber Event	2. Cyber Incident
3. Cyber Threat	3. Penetration Testing
4. Data Breach	4. Vulnerability Assessment
5. Denial of Service	
6. Indicators of Compromise	
7. Information Sharing	
8. Insider Threat	

* In the consultative document, 'insider threat' was a proposed new term and a revised definition for Cyber Incident was proposed.

No revisions were applied to eight terms for the following reasons:

- 'Cyber event' is already defined, and the current definition was deemed sufficient.
- 'Compromise', 'Denial of Service', 'Data Breach' are already defined and no concrete proposals were advanced, therefore no action was implemented in response to those proposals.
- 'Cyber Threat' is already defined, which is aligned to the definition for cyber attack. The respondent's proposed definition introduced a different meaning than was intended, so this suggestion was not taken further.
- A respondent suggested to include the concept of 'voluntariness' in the 'Information Sharing' definition, which would be restrictive and narrow down its scope. Therefore, the current definition was deemed sufficient, and no further action was taken.
- The proposed revision to 'Insider threat' restricted the definition to trusted entities within an organisation, which would be too narrow and therefore drive unwarranted exclusions (e.g. contractors).
- It was also proposed to add examples such as 'File names/hashes, process names, registry entries' to the definition of 'Indicators of compromise'. However, as definitions should be comprehensive and not rely on examples, no change was implemented.

Four terms were revised as follows:

- **Cyber Alert**. The current definition of cyber alert is complemented by adding a second meaning, to recognise that the term can denote two separate concepts which are both deemed to be significant in the realm of cybersecurity. The second added definition is 'Announcement of an abnormal situation or condition (from one or more cyber events) requiring attention', adapted from ISO 8468 2007 (Announcement of an abnormal situation or condition requiring attention).

- **Cyber Incident**. Sub-criteria (ii) ('violates the security policies, security procedures or acceptable use policies') was removed from the definition as this was seen as a redundant requirement, given that any violation of security policies or procedures that would adversely affect the confidentiality, integrity or availability of the information system would already be captured in the first part of the definition. There were also mixed views from respondents over whether the definition should be kept broad to encompass incidents arising from both malicious and non-malicious activities, or to confine it to focus only on malicious activities. Given that most financial authorities have been using the term more broadly in their policies, regulations and/or guidance, the FSB decided that the broader definition should be adopted to promote convergence in CIR. A detailed explanation of the key concepts that underpin the definition of 'cyber incident' has been included in the revised Cyber Lexicon in an Annex.

- **Penetration Testing**. The phrase 'using all available documentation' has been removed from the definition to make term more broadly applicable. The previous definition included test conditions where all available information is shared with testers (historically referred to 'white box' testing), but excluded tests where limited or no information is provided (formerly 'grey box' or 'black box' testing).

- **Vulnerability Assessment**. The word 'product' was included among the list of objects subject to the systemic examination in the definition of vulnerability assessment. The merit of this choice is the possibility to carry out the assessment on assets which do not yet form part of an information system but can be subject to a vulnerability assessment.

3. Format for Incident Reporting Exchange (FIRE)

The overarching tone of responses conveyed universal, but occasionally conditional, support for the initial FIRE concept. Although the proposals were considered to be clearly presented, some respondents sought further information and clarity on how FIRE would be taken forward. In addition, a subset of comments strayed into implementation concerns which relate to how FIRE could be used rather than FIRE itself.

The following four sections summarise key observations arising from the consultation questions related to FIRE which will inform the project's future.

3.1. Would FIRE contribute to greater convergence?

There was general consensus across responses that the FIRE concept could facilitate greater convergence. In some cases, respondents expressed a desire for it to go beyond the bounds of the FSB's mandate, by either directing authorities to adopt FIRE to promote standardisation or seek broader harmonisation beyond the financial sector. To be successful, some respondents also stressed that the implementation of FIRE would ultimately need to demonstrate greater simplification or de-duplication of the incident reporting landscape.

Specific comments from individual respondents have also been acknowledged, including:

- information requirements for initial reporting should strive to be simple, high-level, and actionable, which is in line with CIR Recommendation #4 on phased and incremental reporting;

- the concept of 'accumulating events' could be incorporated within the related event concept referenced in the consultative report, which could be further explored in the design of FIRE; and

- the implementation of any common reporting format could have a disproportionate impact on small- and medium-sized FIs when implementing changes to reporting regimes.

Suggestions which were not taken forward include: (i) the standardisation of reporting thresholds, which are explicitly decoupled from the reporting format; and (ii) the exclusion of relative incident severity or lessons identified, as this information is considered to be of relevance and value to financial authorities.

3.2. Is the FIRE concept readily understood?

Although most respondents indicated that the FIRE proposal was clearly understood, subsequent references within responses suggested different interpretations on the final form of FIRE. To clarify, FIRE is not intended to be a tool, portal, system, form or (centralised) database, but is a human and/or machine readable expression of the information requirements for exchanging incident reports.

Many respondents also sought further details or clarity on the role of financial authorities in the FIRE lifecycle, ownership and funding model. It is expected that these aspects would be addressed once the project commences. Another recurring theme was the inclusion of security requirements which would be handled outside of FIRE as part of local implementations, following the guidance set out in CIR Recommendation #16. A number of comments were received in regard to the inclusion or treatment of specific data fields which would not be assessed until the FIRE design phase.

One respondent requested further clarity on use of FIRE for authority-initiated reporting. FIRE is not intended to draw information directly from SOCs within FIs, but instead initiates a request from financial authorities to FIs to provide incident reporting information during sector-wide incidents.

3.3. Who should be involved in FIRE development?

In addition to collaboration between financial authorities and FIs, respondents suggested a variety of possible stakeholders to involve in the development of FIRE, including:

- representation from sectors upon which FIs rely (e.g. telecoms, energy, technology);

- financial sector trade associations;

- national cybersecurity agencies (e.g. ENISA, CISA);

- other non-financial sector authorities (e.g. data protection);
- CERTs or ISACs; and
- the vendor community.

One respondent suggested that entities with specific subject matter expertise or past experience could be consulted as part of the development process. Another respondent also suggested engaging with a selection of critical third party providers (CTTPs), particularly if they may be directly subject to incident reporting requirements from financial authorities in future as new CTTP regimes emerge.

3.4. What are the necessary preconditions for FIRE?

The most cited precondition by respondents is understanding the interaction between FIRE development and similar concurrent efforts across G20 jurisdictions (e.g. development of Level 2 acts for incident reporting as part of DORA). Given their differing scopes and the intrinsic optionality for FIRE adoption, the project may explore regular exchanges between relevant parties, and potential for collaboration to identify common solutions to shared problems.

Additional individual responses that identified or reiterated pre-requisites for project success include:

- undertaking a thorough analysis of existing incident reporting requirements;
- maintaining flexibility for local implementations;
- establishing common taxonomies e.g. for incident classification;
- measuring the extent to which the sources of operational challenges are addressed; and
- limiting variability in the final design, whilst maintaining a balance between consistency and flexibility.