FSB FINANCIAL STABILITY BOARD

Format for Incident Reporting Exchange (FIRE)

A possible way forward

13 April 2023

The Financial Stability Board (FSB) coordinates at the international level the work of national financial authorities and international standard-setting bodies in order to develop and promote the implementation of effective regulatory, supervisory and other financial sector policies. Its mandate is set out in the FSB Charter, which governs the policymaking and related activities of the FSB. These activities, including any decisions reached in their context, shall not be binding or give rise to any legal rights or obligations.

Contact the Financial Stability Board

Sign up for e-mail alerts: www.fsb.org/emailalert
Follow the FSB on Twitter: @FinStbBoard
E-mail the FSB at: fsb@fsb.org

Table of Contents

Introduction 5
1. Potential benefits, risks and costs 6
    1.1. Potential benefits 6
    1.2. Potential risks and costs 8
2. Planned way forward 9
Annex A: The FIRE concept 10
Annex B: Concurrent efforts within G20 jurisdictions 17

Introduction

As part of its work to achieve greater convergence in cyber incident reporting (CIR),[1] the Financial Stability Board (FSB) found that there is a high degree of commonality in the types of information that authorities require financial institutions (FIs) to report under existing CIR frameworks. Seeing potential to leverage on these similarities to explore greater convergence, the FSB consulted on a concept for developing a common format for incident reporting exchange (FIRE) to collect incident information from FIs and that authorities could use for information sharing. The responses to the public consultation[2] indicated broad, but occasionally conditional, industry support for the FIRE concept.

The FIRE concept is proposed as an approach to promote common information elements and requirements for incident reporting, whilst remaining flexible to a range of implementation practices. Such a format would not require strict global convergence and could be flexible to consider co-existence. Authorities could decide the extent to which they wish to adopt FIRE, if at all, based on their individual circumstances. For instance, authorities could consider leveraging a subset of the features or definitions, which would promote a limited form of convergence. Even if not adopted by a single jurisdiction, FIRE could serve as a common baseline for FIs to map against a range of reporting requirements and assist in translating between existing frameworks.

In terms of scope, FIRE could address information requirements where the practical issues are most acutely observed – for incident reporting initiated by FIs (the most common form of incident reporting requirements). As noted in the FSB 2021 stocktake,[3] the majority of authorities do not distinguish between broader operational incidents and cyber incidents as part of their incident reporting regimes. Therefore, FIRE could cover all forms of operational incidents, not just cyber incidents. to support greater convergence.

Given the implications for the financial sector, the FSB could use its convening power to bring together financial authorities, regulated FIs and other relevant parties to develop FIRE, leveraging incident reporting experience from across sectors and border, and taking into account similar and related efforts to avoid unnecessary duplication (see Annex B). Long-term ownership and maintenance of FIRE would need to be addressed by key stakeholders, preferably at the outset, as a critical factor for the project's overall success and sustainability.

This report reflects the public feedback received on the FIRE concept. Specifically, the potential benefits, risks and costs (Section 1 of this report) and the FIRE concept (Annex A) were updated in response to the consultation. Section 2 discusses how the FSB will take forward the development of FIRE. A detailed workplan will be developed by this summer.

---

1 FSB (2023a), *Recommendations to Achieve Greater Convergence in Cyber Incident Reporting*, April

2 FSB (2023b), *Achieving Greater Convergence in Cyber Incident Reporting: Overview of responses to consultative document*, April

3 FSB (2021), Cyber Incident Reporting: Existing Approaches and Next Steps for Broader Convergence, October.

1. Potential benefits, risks and costs

1.1. Potential benefits

FIRE would be designed to realise several benefits[4] for both financial authorities and FIs, including:

- **Flexibility for implementation by authorities**. The FIRE concept would be designed with flexibility at its core, to allow for a degree of adaptation to suit local needs, and potential future innovation in incident reporting requirements. For example, FIRE would:
  - strike a balance between shared structured fields which limit variability in reporting and drive universal consistency, versus open fields which individual authorities can issue bespoke guidance against as part of their local implementation to fulfil their unique information needs;
  - include the concept of field optionality, by defining the minimum data requirements which individual authorities can exceed;
  - allow individual authorities to customise field and parameter names to support multi-lingual variants or equivalent local terminology;
  - focus on message content, and not prescribe how reporting messages are generated or handled on receipt; and
  - remain agnostic to individual authorities' reporting thresholds.
- **Addressing sources of operational challenges**: If developed successfully, the FIRE concept has the potential to reduce the operational challenges on FIs by furthering greater convergence in the following areas, thereby enabling FIs to devote a greater proportion of resources to resolving incidents and addressing their causes:
  - *Definitions*: By adopting terminologies in the Cyber Lexicon[5], FIRE would bring about consistency of terminology used as part of incident reporting.
  - *Information requirements*: FIRE encapsulates a single, but flexible, set of data fields that could satisfy the reporting needs of multiple authority stakeholders. However, complete coverage of all data fields to create a superset of all existing authority reporting requirements would not be practical, nor necessary to achieve the key benefits of the proposal.

---

4 The benefits listed would in most cases not be fully realised, and therefore not be measurable, until critical mass adoption of FIRE had occurred. Hence, these benefits form part of a broader set of critical success factors which span beyond this project into implementation and deployment.

5 FSB (2023c), *Cyber Lexicon: Updated in 2023*, April

- *Classification schemes*: The standardisation of field options and taxonomies that underpin structured data fields, such that all users of FIRE have the same reference point.

- *Multiple recipients*: An ability to support one-to-many communication of incident reports (subject to technical implementation).

- *Mechanisms*: It may be possible to coalesce towards common mechanisms for sharing incident information.

- **Improving capabilities to support reporting objective**. FIRE has the potential to streamline comparative and analytical capabilities which leverage incident data sets.[6] In particular, the structured elements of a common reporting format facilitate the ability to compare and contrast incident occurrences on a historical, cross-border or cross-sectoral basis. These attributes could be of particular benefit in conducting more systematic analysis of reporting to identify trends or common root causes for industry feedback purposes or to facilitate stronger cross-border cooperation through a common understanding of an incident as it is reported.

- **Enabling automation**. The standardisation proposed within FIRE may facilitate a reduction in manual overheads within existing reporting processes through the introduction of automation, thereby generating further efficiencies:

  - *Machine generated*: FIs could automate the extraction of information directly from their internal incident management systems to generate FIRE messages with no/little additional burden.

  - *Machine readable/actionable*: Financial authorities could take in information received without resorting to manual handling, creating a frictionless process for FIs to communicate with authorities.

- **Resource efficiency**. Rather than individual authorities expending resources to solve a common problem, FIRE represents a collaborative endeavour that can benefit from the collective knowledge and experience from all participants, to produce an output usable by all. Those authorities not directly involved in the development of FIRE, and who are yet to establish their own reporting format requirements, would be able to leverage the final product without incurring the associated costs. Furthermore, financial authorities and FIs may be able to implement common reporting solutions which are subsequently developed to support FIRE.

- **Fostering ecosystem-level change**. To instigate change on a larger scale, the initiative would also benefit from supporting solutions for small or mid-sized FIs that may not have the in-house capability to implement FIRE. For this end of the market, it is possible that third-party providers of incident management services or products could engineer their systems to support FIRE, thereby promoting greater utility across the financial

6 FSB (2023a), Annex A, Section 2.

ecosystem. To that end, it may be beneficial to involve this stakeholder group as part of the design team, such that these solutions could be made available early in the process. Additionally, convergence in institution-initiated incident reporting may lead similar information requirements propagating through supply chains to support reporting of incidents to FIs by their third parties. Although not currently in scope, the potential for FIRE to be used in this context could be investigated.

1.2. Potential risks and costs

A transformation programme of this magnitude does not come without risk and costs, and requires the investment of time, effort and resource to fully realise its potential. Potential sources of risk and costs which could halt or impede this proposed initiative or diminish its intended benefits are summarised below.

Potential risks

- **Lack of project sponsorship**: Failure to gain sufficient cross-stakeholder support and commitment to multi-year transformation programme.
- **Insufficient adoption levels**: Whether by choice or based on circumstance, the failure to attain critical mass and thereby confer maximal benefits is not achieved.
- **Localised mismatch in appetite**: Decision not to proceed by a financial authority may be locally challenged by FIs that have a greater desire for uptake. In the same way, decision to proceed by an authority with an already established notification framework and format may be perceived by FIs as an unnecessary effort.
- **Irreconcilable design positions**: Divergent views over time on design of elements of FIRE may reduce degree of convergence, or lead to competing approaches. Divergent views may also be intrinsically tied to domestic reporting obligations linked to national/state incident reporting requirements (not just cyber).
- **Long-term maintenance risk**: Ownership and the process for future development of FIRE would need to be determined.

Potential costs

- **Transition arrangements**: Financial authorities may have to support both pre-existing and FIRE-based receipt of incident reporting information whilst regulated FIs migrate.
- **Policy adjustments**: There may be implementation costs involved in changing existing regulatory policies and rules to support implementation.
- **Unappealing 'cost of entry'**: The overall one-off costs involved with implementation and migration may be less palatable than the current recurring overhead of operational challenges, or the costs could be too high and prohibit adoption. Additionally, these costs may be unevenly borne across the sector, particularly in smaller, less complex FIs with fewer resources to implement these changes.

2. Planned way forward

To take this work forward, the FSB will establish a new working group comprised of financial sector authorities under the FSB Standing Committee on Supervisory and Regulatory Cooperation (SRC). The development of FIRE is expected to take place over several phases, and over the course of up to two years:

- **Mobilisation**: Identifying public and private participation and project resources, and forming the working group and its associated terms of reference.
- **Discovery**: Identifying stakeholder needs, pre-requisites, and feasibility.
- **Design**: Designing options which seek to fulfil these needs.
- **Consultation**: Public consultation on the identified options.
- **Publication**: Finalisation of the report, reflecting public feedback, which may include both human and machine-readable formats.

Throughout this process, the working group will collaborate with industry, including interested stakeholders outside of the financial sector, as well as authorities beyond the FSB membership (see Box 1).

Box 1: Examples of stakeholder types

The potential stakeholder groups compiled below represent a non-exhaustive list of parties which may be involved or engaged as part of the FIRE project.

Authority stakeholders

- FSB Member Authorities
- Non-FSB Member Authorities
- FSB Regional Consultative Groups (RCGs)
- International Organisations
- Financial Standard Setting Bodies
- National Cybersecurity Authorities

Industry stakeholders

- Regulated FIs
- FS Trade Associations / Collective Forums
- Technology Service Providers
- Non-FS Sector (telecoms, energy)

Annex A: The FIRE concept

Initial views on the FIRE concept have been limited to institution-initiated reporting, though other reporting types may also be incorporated. Importantly, the ideas conveyed in this section should be viewed as seed material for future discussions as to how a concept might be constructed.

In addition, a text-based articulation of data requirements, with their accompanying formatting and logic rules, may be open to misinterpretation. To eliminate this interpretation risk, it may be necessary to encode the final concept into one or more commonly used data interchange formats such as JSON or XBRL which will also facilitate technical implementation.

Concept structure

To determine an appropriate organising structure for the information requirements within the proposed concept, a 'meet in the middle' approach was used to inform the overall structure:

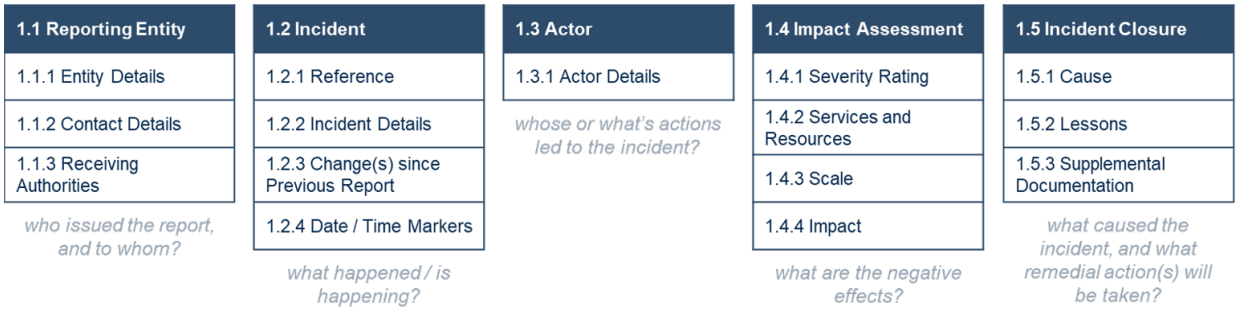
- **Bottom-up**: using the results of the granular data field mapping exercise performed on existing reporting templates, which identified the minimum set of common types of information.
- **Top-down**: pooling information requirements with a common purpose.

By grouping common data requirements, clear patterns of overlap emerged upon which the premise of this concept was founded. The decision to initially focus FIRE design on institution-initiated reporting was based on: (i) being the most common reporting type implemented by authorities; and (ii) where the practical issues were most commonly observed.

Although specifics vary, the underlying premise for institution-initiated reporting is shared by all authorities, i.e. a FI experiences an incident which, depending on the circumstances, triggers a reporting obligation to one or more receiving authorities. The nature of the information flows is event-driven, and unidirectional from the reporting entity to the receiving authorities. Depending on individual reporting requirements, more than one incident report may need to be issued for the same incident.

From the top-down viewpoint, the information requirements for institution-initiated reporting were grouped into five distinct collections (as shown in Figure 1). Collectively, these data fields provide receiving authorities with the necessary information to understand incidents as they evolve, and to act accordingly. The data fields are also linked to the report phasing concept, whereby required elements are limited to those deemed essential for any given phase, e.g. such that information collected through initial reporting remains simple, high-level, and actionable. Each of the subsequent subsections elaborates on each collection, and the types of information which could be defined in a future concept design.

Breakdown of group data fields for institution-initiated reporting **Figure 1**



Reporting Entity

The data fields associated with the reporting entity are intended to describe:

- **Entity Details**. The data fields under consideration contain basic referencing and classification information for the reporting entity. With the exception of the entity name, which reflects the entities legal or most commonly used designation, the remaining fields are structured to support analysis across the reporting entity data set, within and across reporting authorities. Identification schemes could support both global mechanisms (e.g. legal entity identifier (LEI))[7] and pre-existing local implementations. For entity type, there is a design choice between: (i) using existing classification schemes (e.g. International Standard Industrial Classification)[8] that can act as an authoritative reference source but may be insufficiently granular; and (ii) developing a bespoke classification scheme which provides maximum flexibility. Basic information could also include reference to the country where the affected entity is domiciled.

- **Contact Information.** Designated points of contact within entities are typically required in case a receiving authority requires further information following the submission of an incident report. FIRE therefore would need to support the capture of contact information for those representatives.

  As the use of single or multiple contacts varies across existing incident reporting arrangements from different authorities, FIRE would need to support the submission of one or more contacts, with the ability for the receiving authority to implement in line with their local needs. Although fields such as role or department could be considered optional, the contact's email address and phone numbers may be viewed as required fields, such that authorities have two methods of communication to reach the entity's representative(s).

---

7 The LEI is a 20-character, alpha-numeric code based on the ISO 17442 standard developed by the International Organization for Standardization (ISO). It connects to key reference information that enables clear and unique identification of legal entities participating in financial transactions. Each LEI contains information about an entity's ownership structure and thus answers the questions of 'who is who' and 'who owns whom'.

8 UN Statistics Division (2008), *International Standard Industrial Classification (ISIC) of all Economic Activities, Revision 4.*

- **Receiving Authorities**. FIRE could include data fields to support potential use cases related to the delivery and routing of incident reports, such as:

  - the ability for a reporting entity to send the same incident report to multiple receiving authorities simultaneously, thereby driving one-to-many efficiencies;

  - maintaining a record of authorities that have previously received reports regarding the same incident, but not the current incident report instance being issued; or

  - facilitating onward sharing of an incident report to other authorities who have not been informed of the incident directly by the affected entity (assuming appropriate information-sharing arrangements are in place).

To reference authorities within these fields, the use of common authority abbreviations may be desirable for brevity and standardised encoding. At this time, an authoritative source of financial authority identifiers is not established and may need to be defined as part of FIRE. One possible suggestion would be to combine ISO 3166 alpha-2 country codes[9] with the locally recognised acronym for the authority to maintain uniqueness (e.g. US Federal Reserve Board is encoded as 'US-FRB'). In addition, a future iteration of FIRE may wish to support onward sharing beyond financial authorities to other authorities.

Incident

The following data fields consolidate information requirements related to the incident being reported, such as entity- or authority-generated unique identifiers for the incident being reported, or other incidents which may be related; the nature and circumstances of the incident, which are augmented and refined as the incident evolves; actions taken or reactions to the incident which have transpired since the previous incident report; and information on timing for key incident milestones.

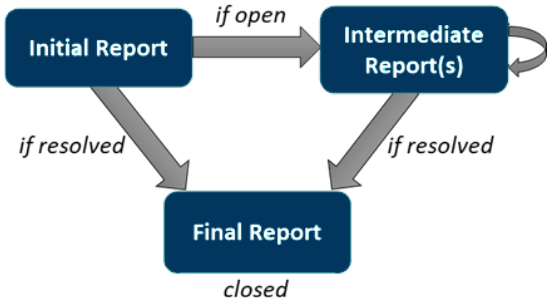
- **References**. To support the tracking of individual incidents, and possible interdependencies, FIRE may need to include multiple identifying reference fields which serve different purposes. These fields could include the unique identifiers used internally by the reporting entity to refer to the incident or any related incidents (e.g. a sector-wide cascading incident). Equally, FIRE may need to store authority-generated references used to identify a reported incident or create relationships between incidents reported by multiple entities. When combined with onward sharing between authorities, the entity-provided identifiers could act as a unique key across authorities when engaging with the reporting entity, on an individual or collective basis.

- **Incident Details**. This section describes potential base attributes for an incident, which could include: the phasing of incident reports and related incident status (as shown in Figure 2); the incident's title and description which provide an overall reflection of the incident at differing levels of granularity; the type of incident, which reflect the event which has occurred in a cause-agnostic manner; the method by which the affected

9 ISO (2020), *ISO 3166 Country Codes.*

entity became aware of the incident; the confidence level which the reporting entity has in the information provided within the report; the criteria which triggered the reporting obligation; and an estimated time of resolution for when the incident is expected to be brought under control.

Report type workflow and valid states **Figure 2**



	Initial	Intermediate	Final
Open	✓	✓	✗
Resolved	✓	✓	✗
Closed	✗	✗	✓

- **Change(s) Since Previous Report**. Whereas the previous section on Incident Details seeks to capture the evolving nature of the incident, potential data fields within this section have been grouped together to reflect new incident developments that have arisen between reports (or as part of the initial report if applicable). These could include: actions taken by the reporting entity to bring the incident under control, such as interim procedures and solutions; the level of internal escalation involved in response to the incident; a summary of the public reaction; the issuance of external communications; and the names of any other non-financial authorities or agencies notified.

- **Date/Time Markers**. Incident information often contains markers that reflect the specific timing of milestones within an incident. In addition to the four common incident time markers (occurrence, detection, resolution and closure), FIRE could also capture the time at which a specific report was issued, and an estimate for the timing of the next report to manage authority expectations.

Actor

Alongside capturing the nature of the incident, FIRE could also contain fields to record the identity of the parties or forces (referred to as actors herein), whose actions led to the incident. The use of the term 'actor' is broader in scope than the Cyber Lexicon's definition of a 'threat actor' which represents '*an individual, a group or an organisation believed to be operating with malicious intent*', so as to include parties which do not have intent. Possible fields include a classification scheme for the type of actor (inclusive of internal, third party and external[10] actors), the actor's identity (where known and appropriate), their country of origin, motivation, and whether their actions were directly or indirectly targeted at the reporting entity (or were untargeted altogether), and any supplemental information that may be actor-specific (e.g. identifying indicators such as IP addresses).

[10] An external actor has no pre-existing relationship with the reporting entity, which differentiates it from third-party.

As incidents may involve the actions of more than one actor, FIRE may need to support the submission of all of the attributes for individual actors. For example, multiple threat actors could combine forces to achieve common objectives where interests align.

Impact Assessment

Consequences arising from incidents are typically expressed in the form of impact, which is defined by ISO[11] as the '*outcome of a disruption affecting objectives*'. However, the measurement of impact involves the study of lagging indicators that can only be collected after an incident occurs, and which may not be immediately discernible. Therefore, the evaluation and articulation of impact for incident reporting purposes, especially in the early stages, has to be grounded in what is known or readily observable. Hence, the suggested fields related to impact are grouped and ordered to reflect the sequence by which reporting entities might assess them.

- **Severity Rating**. Whereas impact assessment is seeking to evaluate the consequences of an incident with an outward focus, the notion of severity provides an indication of the significance and urgency which the reporting entity places on addressing the incident. The approaches to severity used by entities and authorities are typically tailored and therefore idiosyncratic to each entity.

  This source of uniqueness presents a dilemma with two opposing drivers: achieving greater convergence to enable cross-entity comparability, whilst respecting individual entity choices and diversity across the ecosystem.

  In order to strike an appropriate balance, it may be necessary for FIRE to capture both the reporting entity's internal reference of the incident's severity on its own terms (including supporting definitions), and a normalised interpretation of the reporting entity's severity set by the receiving authority. The approach eventually taken will ideally seek to promote a degree of normalisation, without forcing homogeneity as an outcome.

- **Services and Resources.** Although the circumstances may not be fully understood at the outset of an incident, the reporting entity will likely be able to rapidly develop a reasonable understanding of the technical impacts to its services and underlying resources. As such, this information could be considered as the next grouping of data fields that can build towards an overarching impact assessment. Aspects of service and resource type, the nature of their criticality to the entity, and the type of disruption experienced could all be captured in this section of FIRE.

- **Scale**. As impacts propagate beyond the reporting entity, an understanding of which parties may be affected (and to what extent) gradually emerges based on either the entity's own knowledge, or as communicated by affected parties. To collect a consistent expression of the scale of an incident, FIRE could focus on measures typically found in

[11] ISO (2021), *ISO 22300:2021 – Security and resilience – Vocabulary*.

existing reporting implementations, such as affected customer/consumer base, transaction volume, other parties affected and geographic spread.

- **Impact**. The assessment of impact is a non-trivial task, requiring an evaluation of the consequences of an incident over multiple time horizons, ranging from short-term (intra-day) to long-term (months, even years). Quantitative approaches are generally more challenging for individual entities to initially define and source accurate and timely data to use as part of incident response. Therefore, FIRE may be designed to use a qualitative approach to evaluating impact which can more easily be applied across all types of reporting entities.

  This judgement-based method could use descriptive statements to define levels of increasing severity across a range of impact categories (e.g. financial, operational, reputational, legal/regulatory). Over the course of an incident, a reporting entity may perform regular appraisals against these qualitative scales to approximate impact and to drive appropriate organisational responses. However, this approach relies on consistent interpretation and judgement of individuals who may introduce bias or subjectivity. It may therefore be necessary to introduce a normalised set of impact scales, although the intent is not to supplant existing levels defined by either reporting entities or receiving authorities. Instead, the scales could provide a common form of intermediation to enable comparability of impact across incidents.

Incident Closure

The fifth and final set of data fields related to institution-initiated reporting are confirmed once the incident has been resolved and a post-incident review performed. Therefore, these information requirements are intended for the content of the final report, though certain elements may be suspected or known even in the early stages of an incident. There are three key elements: cause, which explains why the incident took place; lessons identified and remedial activity, which detail any vulnerabilities and actions to be taken to address them; and supplemental documentation to enable inclusion of file-based supporting materials, such as detailed analysis of the incident.

- **Cause**. During the incident response phase, the primary focus is on bringing the situation under control and restoring service provision to acceptable levels. Therefore, an in-depth analysis of causation will typically not occur until during a post-incident review. However, the reporting entity may have developed a good understanding of the incident's cause(s) as part of its response, and therefore may be able to provide receiving authorities with early insight whilst the incident is still in progress.

  Types of causes that could be considered for FIRE include hazards (natural and man-made), causal factors arising from human performance, information system and process failures, external dependency failures, and threat vectors for malicious acts. In addition, FIRE could capture the causal strength associated with each cause identified which could range from contributory to strongly causal (i.e. must have led to the incident).

- **Lessons**. Following root cause analysis, a post-incident review is expected to identify one or more lessons for the reporting entity to take actions against. Note the use of ‘lessons identified’ as the product of a post-incident review, rather than the more commonly used ‘lessons learnt’. Identified lessons subsequently need to be implemented or applied, and then engrained within an entity before they can be considered as learnt. A combination of each lesson, associated remedial action and estimated completion date for each action, could provide both the reporting entity and receiving authority with the necessary remediation planning information to monitor progress and to subsequently evaluate whether root causes have been adequately addressed.

- **Supplemental Documentation**. As not all information can be captured through structured text-based fields, FIRE may need to include a mechanism for including file-based materials as part of any incident report. Although primarily to support detailed information related to post-incident reviews, it is conceivable that receiving authorities may wish to have additional content submitted at other points in the incident lifecycle.

Annex B: Concurrent efforts within G20 jurisdictions

Incident reporting is the subject of active policy development and issuance across a number of G20 jurisdictions, which are likely to overlap with the outputs of the FIRE project. Given the differing scopes and intrinsic optionality for FIRE adoption, the emphasis should be on regular interactions between relevant parties, and potential for collaboration to identify common solutions to shared problems.

The following jurisdictional activities have been highlighted due to their significance, relevance, and overlapping timeframes with the FIRE project.

European Union

As part of the broader EU Digital Finance Package[12], the Digital Operational Resilience Act (DORA) institutes a dedicated framework to safeguard digital operational resilience for finance. Entering into force on 16 January 2023 before becoming applicable on 17 January 2025, the DORA regulation is to be supplemented by numerous Level 2 acts, including those with relevance to incident reporting:

- **Classification of ICT-related incidents and cyber threats** (Article 18), whereby the European Supervisory Authorities (ESAs), in consultation with ENISA, are to submit a draft text of a Regulatory Technical Standard (RTS) to the European Commission by 17 January 2024. With public consultation expected between June and September 2023, the RTS should specify:
  - Materiality thresholds for major ICT-related incidents;
  - Criteria for competent authorities to assess the relevance of incidents; and
  - Detail of incident reports (considering international standards, and guidance / specifications by ENISA, including, where appropriate, for other sectors).
- **Harmonisation of reporting content and templates** (Article 20), whereby the ESAs, in consultation with ENISA, are to submit a draft text of a RTS to the European Commission by 17 July 2024. With public consultation expected between November 2023 and February 2024, the RTS should specify the content of:
  - major ICT-related incident reports (including timing for initial reporting); and
  - notification of significant cyber threats.

  Additionally, the ESAs shall consider specificities of the financial sector and provide justification when deviating from NIS2 (e.g. on timelines).

[12] European Commission, *Digital Finance*

United Kingdom

The Bank of England, Prudential Regulatory Authority (PRA), and Financial Conduct Authority (FCA) have jointly committed to reviewing regulatory incident reporting[13]. Separately, on Outsourcing & Third Party (OATP) Reporting, the PRA has also committed to consult on proposals to collect information on firms' material OATP arrangements. Due to the similarities across both collections, incident and OATP reporting elements have subsequently been combined into a single project (IOREP).

In April 2022, the IOREP project was formally included as a pilot use case within the Bank/FCA **Transforming Data Collection (TDC)[14]** programme, which seeks transform regulatory data collections over the next decade, such that *'authorities obtain the data that they need to fulfil their missions at the lowest possible cost to industry'*. The TDC initiative is also a joint endeavour with industry, where collaboration on both design and implementation is incorporated from the outset. Through the TDC programme, the UK supervisory authorities are seeking input on:

- supporting the development of formal Incident and OATP Reporting policies;
- standardising information FIs submit to financial authorities; and
- end-to-end service design, development and implementation of any reporting solution.

As of February 2023, the IOREP project is underway, with joint Bank/PRA/FCA consultations on Incident and OATP Reporting currently scheduled for Q4 2023.

United States

In February and March of 2022, the Securities and Exchange Commission (SEC) proposed amendments to its rules to enhance and standardise disclosures regarding cybersecurity risk management, strategy, governance, and incident reporting by investment advisers, registered investment companies, business development companies and public companies. The proposed amendments would require, among other things, current reporting about material cyber incidents and periodic reporting to provide updates about previously reported cyber incidents.

Also in March 2022, the US President signed into law the Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA). CIRCIA includes a number of requirements related to the required reporting and sharing of covered cyber incidents. Notably, CIRCIA requires the Cybersecurity and Infrastructure Security Agency (CISA) to develop and issue regulations requiring covered entities[15] to report to CISA any covered cyber incidents within 72 hours from

---

13 Commitments made: (i) to the UK's Treasury Select Committee; (ii) within the 2019 Operational Resilience consultation CP29/19; and (iii) as published in supervisory authority business plans.

14 Bank of England, *Transforming Data Collection*

15 In developing a definition of "covered entity", CIRCIA requires CISA to consider three broad factors: (i) the consequences that a particular cyber incident might have on national or economic security, public health and safety; (ii) the likelihood that the entity could be targeted for attack; and (iii) the extent to which an incident is likely to disrupt the reliable operation of critical infrastructure.

the time the entity reasonably believes the incident occurred. On 12 September 2022, CISA issued a request for information seeking public input on a number of topics, including:

- Definitions of and statistics pertaining to various terms to be used in the proposed rules, including the scope-defining terms "covered entity," "covered cyber incident," and "substantial cyber incident;"
- The form, manner, content, and procedures for submission of cyber incident (and ransom payment) reports required under CIRCIA, including initial reports and follow-ups;
- The criteria for what constitutes a "reasonable belief" that a covered cyber incident has occurred, triggering the 72-hour deadline to report such incidents;
- Information regarding existing federal or state incident reporting requirements and potential areas of overlap or conflict between those requirements and CIRCIA; and
- The typical time and costs needed to comply with existing incident reporting requirements.

As part of the rulemaking process, CIRCIA requires CISA to publish a Notice of Proposed Rulemaking (NPRM) within 24 months of the enactment of CIRCIA (i.e. no later than March 2024), and to issue a Final Rule setting forth the regulatory requirements within 18 months of the publication of the NPRM.