FSB FINANCIAL STABILITY BOARD

Format for Incident Reporting Exchange (FIRE)

Consultation report

17 October 2024

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 X/Twitter: @FinStbBoard
E-mail the FSB at: fsb@fsb.org

Questions for consultation

The Financial Stability Board (FSB) invites comments on this consultation report and welcomes replies to the questions set out below. Responses should be submitted via **this online form** by 19 December 2024.

Responses will be published on the FSB's website unless respondents expressly request otherwise.

Please contact the FSB by email (fsb@fsb.org) if you have questions or if you wish to provide any supplementary material, and mention "FIRE public consultation" in the subject line.

Background

As part of its comprehensive approach to achieve greater convergence in cyber incident reporting,[1] the FSB published in April 2023 a report on a possible way forward for a Format for Incident Reporting Exchange (FIRE). Since then, the FSB surveyed its members and engaged with the private sector to assess the information requirements and feasibility of FIRE. Drawing on the survey findings and an in-depth analysis of commonalities between several existing reporting frameworks, the FSB proceeded to design FIRE to promote convergence, address operational challenges arising from reporting to multiple authorities and foster better communication.

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. *(Free-text)*

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. *(Free-text)*

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? *(Free-text)*

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

[1] See the FSB press release, April 2023.

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? *(Free-text)*

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.

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

Table of Contents

Executive Summary

Since 2017, the Financial Stability Board (FSB) has underscored the threat of cyber incidents to the stability of the financial system. Effective incident response and recovery are crucial to mitigating financial stability risks. The FSB is working to identify and address weaknesses that could exacerbate such shocks.

Incident reporting is a key mechanism for financial authorities to monitor disruptions within regulated entities. Differences in reporting approaches across jurisdictions result in fragmented requirements and coordination challenges. Greater harmonisation of regulatory reporting supports firms' efficient incident response and recovery, as well as effective supervision and cooperation among authorities. The Format for Incident Reporting Exchange (FIRE) aims to promote common information elements for incident reporting while allowing for flexible implementation practices. Authorities can choose the extent to which they adopt FIRE, and leverage its features and definitions to promote convergence and facilitate translation between existing frameworks.

FIRE is designed to cover operational incidents, including cyber incidents, and extends beyond the FSB's previous work on cyber resilience. It provides a set of common information items for reporting incidents but does not define common reporting triggers, deadlines, or mitigation approaches. The design focuses on financial sector participants' reporting to authorities and is flexible to enable regulated entities to leverage FIRE in their relationships with service providers. To maximise flexibility and interoperability, FIRE contains a data model using the Data Point Model (DPM) method, which allows for machine-readable versions of FIRE such as in eXtensible Business Reporting Language (XBRL).

FIRE was developed in consultation with private sector participants. The process included a Discovery Phase to identify commonalities in incident reporting needs and a Design Phase to develop the components of FIRE. A Testing Phase is underway to validate the design and robustness of FIRE using different incident types and scenarios. After the public consultation, the final version of FIRE is expected to be published by mid-2025, with a workshop planned for 2027 to review experiences and determine the need for revisions.

FIRE's features support flexibility for authorities that adopt the format in full or in part. Of the 99 information items defined, 51 are optional, allowing authorities to decide which to implement based on their needs. Authorities can customise the baseline view of reporting phases, while remaining mindful not to compound operational challenges. They can choose to provide additional specifications for unstructured fields. Moreover, field names and permissible input can be adjusted to support local language needs while maintaining conceptual equivalence.

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 and interoperability benefits.

Introduction

Since 2017, the Financial Stability Board (FSB) has highlighted the threat of cyber incidents to the stability of the financial system and began identifying and addressing weaknesses and inefficiencies that could exacerbate such shocks. Efficient and effective response to and recovery from incidents is essential to limiting related financial stability risks. Greater harmonisation of regulatory reporting supports the effective supervision of financial institutions and facilitates cooperation and coordination amongst authorities in monitoring and addressing these risks.

Incident reporting is considered one of the primary mechanisms used by financial authorities to maintain visibility of disruptions occurring with their regulated entities, and in line with their individual mandates. However, approaches to incident reporting have developed independently over time, leading to fragmented reporting requirements and coordination challenges across authorities and across jurisdictions.[2]

The Format for Incident Reporting Exchange (FIRE) is an approach to promote common information elements and requirements for incident reporting, whilst remaining flexible to a range of implementation practices. It builds on the FSB report on a possible way forward for developing FIRE[3] and aims to address information requirements where the practical issues are most acutely observed. 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 format for financial institutions to map against a range of reporting requirements and assist in translating between existing frameworks.

During the FSB's work on Cyber Incident Reporting,[4] three distinct reporting types were identified, for which the respective information requirements have been reflected in this format:

- **institution-initiated reporting**, triggered when an incident meets the reporting criteria of one or more financial authorities or when reported voluntarily, and includes initial, intermediate, and final reporting associated with end-to-end incident lifecycle;
- **authority-initiated reporting**, where incident information is reported after a request from one or more authorities to better understand the effects of a sector-wide incident; and
- **periodic reporting** of incident-related information gathered from regulated institutions on a regular basis (not event driven).

---

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

3 FSB (2023a), *Format for Incident Reporting Exchange (FIRE): A possible way forward*, April.

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

Given that institution-initiated reporting is the most prevalent type of reporting and poses the greatest operational challenges for financial institutions, the FIRE design has focused on defining common information items for institution-initiated reporting.

The FIRE design is limited to a set of common information items for reporting incidents. It does not define common reporting triggers, reporting deadlines, mitigation approaches or other aspects of cyber incident response and recovery.

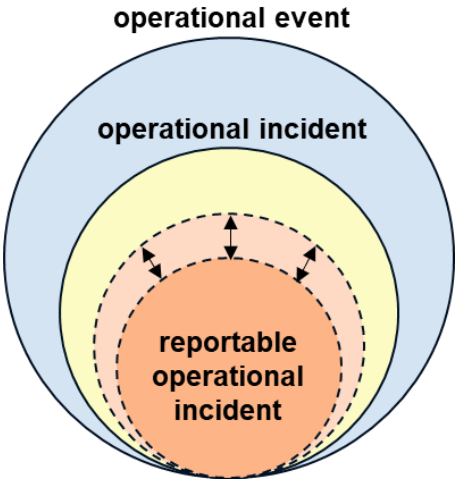
In addition to designing a 'human-readable' format, a data model of FIRE has been developed to maximise flexibility and interoperability using the language-agnostic Data Point Model (DPM)[5] method. This data model enables creating machine-readable versions of FIRE by anyone, such as the one encoded using eXtensible Business Reporting Language (XBRL) that forms part of this consultation package. FIRE provides flexibility to authorities to either leverage the pre-developed XBRL taxonomy (e.g. by requiring xBRL-CSV submissions) or FIRE incident reports in a different reporting language.

Scope of FIRE

The design of FIRE covers reporting of operational incidents (inclusive of cyber incidents), primarily from financial institutions to financial authorities.[6] Previous FSB stocktakes identified that many authorities do not have a different approach or reporting mechanism for cyber incidents specifically. Rather, many frameworks treat cyber incident reporting as part of broader operational incident reporting. For that reason, the scope of FIRE extends beyond the FSB's previous work on cyber resilience.

To establish the boundary for incident types and underlying causes within the scope of FIRE, three additional terms and associated definitions are provided to complement equivalent cyber terminology found in the FSB Cyber Lexicon.[7]

Figure 1: 'Operational' terminology



Term	Definition
Operational	Relating to people, processes, information, *information systems*, facilities, or external dependencies used to deliver one or more activities, functions or services. Source: Adapted from BCBS and Joint Forum

5 ISO 5116. See for more information International Standards Organization (ISO), ISO/TC 68, "What is DPM".

6 For a more detailed description of the relationships between the core concepts outlined in this paragraph, see Annex B of FSB (2023c), *Cyber Lexicon: Updated in 2023*, April.

7 FSB (2023c).

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. Source: Adapted from ISO and NIST (definition of "Event")
Operational incident	An *operational event* that has been determined to have an adverse impact on an entity prompting the need for response and recovery. Source: Adapted from NIST CSF (definition of "Cybersecurity Incident")

The relationship between these terms is illustrated in Figure 1. The figure interrelates these terms to the concept of a 'reportable operational incident', which represents a varying subset of operational incidents that trigger individual reporting obligations.

Detailed reporting by non-financial institutions is not within the primary scope of the FIRE design, but sufficient flexibility is present in the design for possible use by non-financial institutions and authorities in individual jurisdictions.

Financial institutions could also choose to leverage FIRE in their relations with third-party service providers. They may agree with their (chain of) service providers that the latter use FIRE for their reporting to the institution of any operational incidents that impact their ability to deliver agreed-upon services or other obligations.[8]

Development of FIRE

The development of FIRE took place over several phases, spanning an 18-month period of collaborative effort between public and private sector participants.

Following its initial mobilisation to identify resources with representation from FSB member authorities and industry, the working group initiated a Discovery Phase to identify incident reporting needs based on stakeholder feedback, and to determine the pre-requisites and feasibility of FIRE. An information-gathering exercise was conducted to determine the level of support for individual information items, so as to build consensus on those items and gain a clearer view of estimated effort and complexity to carry out the project.

Having demonstrated sufficient consensus and feasibility to meet the working group objectives, the project entered its Design Phase to develop the components of the FIRE concept. The design effort was divided in two: over 80% of the information items were estimated to require little or intermediate design effort (collectively, 'low-effort' information items), while the remaining information items were considered to require 'significant effort'. The former were taken to the design stage immediately, while the design of the significant-effort information items involved multiple rounds of virtual workshops between authority and industry participants to deepen mutual understanding of the design requirements.

[8] FSB (2023d), *Enhancing Third-Party Risk Management and Oversight: A toolkit for financial institutions and financial authorities*, December, section 3.3.

In parallel with the design work, a comparative exercise was performed against several existing and prospective domestic or regional incident reporting frameworks to identify possible needs for adjustments or inclusion of further information items in the FIRE design.

Steps following public consultation

Alongside the consultation process, the working group, with support from industry stakeholders, is also undertaking a Testing Phase to: (i) validate that the FIRE design is fit for purpose using different envisaged incident types/scenarios; and (ii) test the robustness of FIRE through use of sanitised XBRL incident reports to mimic the lifecycle of incident reporting.

The FIRE project is expected to be finalised around mid-2025, reflecting feedback from the public consultation and outcomes from the testing phase.

The FSB will hold a workshop with industry and authorities in 2027 (around two years after FIRE is finalised) to take stock of their experiences with FIRE, including any implementation challenges. This will inform the need for any revisions to FIRE, as well as provide insight into FIRE's overall success ahead of determining the long-term maintenance of FIRE outside of the FSB.

Organisation of this document

The FIRE format is described within this document using the following structure:

- A section detailing the format for institution-initiated reports, containing:
  - Multiple sub-sections grouped by information items with common purpose (as shown in **Figure 3** for institution-initiated reporting).
  - Tables with accompanying text describing each information item, their purpose, syntax, rules or constraints, and at least one example.
  - A colour code for each information item, identifying whether the item is **essential** (reddish orange) and therefore to be included within local implementations, or **optional** (light yellow) where there is optionality for inclusion.
- Supporting annexes contain details of optionality per reporting phase (**Annex B**) and reference tables for specific information items (**Annexes C-P**).

Guidance for implementation

The design of FIRE includes several features to support flexibility for authorities whilst still achieving an aligned outcome:

- information items: Of the 99 information items defined within FIRE, 51 items are not marked as 'essential' in any reporting phase and therefore authorities may decide which (if any) of these additional information items they wish to implement based on their particular circumstances.

- reporting phases: FIRE defines a baseline view of the reporting of individual information items against each reporting phase. Where an information item is marked as 'optional' in a reporting phase, authorities can decide to make it 'essential' in line with their reporting needs. However, in line with the FSB's Recommendations for Cyber Incident Reporting, care should be taken not to compound the operational challenges that reporting entities already face at the outset of incidents.[9]

- language customisation: Authorities can adjust names and definitions of information items, as well as associated taxonomies, to support local language needs or pre-existing terminology within their jurisdiction. However, if authorities wish to maintain alignment with FIRE, adjusted content must retain conceptual equivalence with the content of this document.

- supplemental guidance for unstructured fields: Several information items within the FIRE format make use of short or long text fields which do not have any constraints on usage, aside from field length. Authorities may include supplemental guidance on the nature of the descriptive information they wish to receive through these information items.

To achieve greater convergence yet flexible outcomes, the FIRE design provides flexibility within a lower and upper bound of available options. That said, reporting solutions that are fully aligned with FIRE must:

- include all essential information items;

- generate and/or collect incident reports that meet (or exceed) the baseline optionality requirements across all reporting phases;

- implement information items within FIRE using the same or compatible field types;

- use the enumerated lists as defined within FIRE (or subsets thereof); and

- not include additional information items not contained within the FIRE design, as these introduce local specificities and exacerbate the challenges faced by reporting entities.

Implementations that adhere to only a subset of these alignment pre-requisites may still achieve a degree of coherence and interoperability with other FIRE-aligned solutions but forego the full benefits of convergence.

9 FSB (2023b), Recommendation 4.

Foundational elements for FIRE reports

Underpinning every information item defined within the FIRE format are 16 base field types (described in Annex A), which set out default syntax rules in line with relevant international conventions or standards.

To facilitate common interpretation between reporting and receiving entities, the format defines the following information items that do not relate directly to the incident being reported, but identify the nature of the information being exchanged:

- **Versioning**: describes the version of the FIRE format being used to describe the incident, such that sender and recipient(s) understand which version this report conforms to.
- **Report type**: describes the type of incident report being exchanged. Only institution-initiated is implemented in Version 1.0.
- **Report language**: describes the language localisation used for the information items and underlying definitions e.g. en-GB means English (UK). Further language customisation is possible through use of private subtags, which allow local implementers to specify their own label variants from the language default.
- **Report currency**: describes the currency used for all monetary references within the report.

Information Item	Purpose / Description	Field Type	Additional Syntax & Validation Rules, and Example Data
FIRE version	Version of FIRE format that message is conformant with	Decimal	**Syntax** • Represented by a decimal number, with at least one decimal place **Validation** • Must be greater than zero **Example** (fictitious) • *1.0*
FIRE report type	Type of FIRE incident report, which determines the fields contained within the rest of the message	Enumerated	**Syntax** • Text (short) enumerated list with one of the following values: ○ Institution-initiated **Example** (fictitious) • *Institution-initiated*
FIRE report language	Language used by report to support localisation	Text (short)	**Syntax** • In line with Internet Engineering Task Force (IETF) Best Current Practice #47[10], language tags are a typically a combination of ISO 639 language

[10] Internet Engineering Task Force (2009), *Best Current Practice #47*

Information Item	Purpose / Description	Field Type	Additional Syntax & Validation Rules, and Example Data
			codes[11] and ISO 3166 alpha-2 encoding country codes[12], separated by a dash. • In addition, to support label customisation by receiving entities, private use subtags can optionally be added using the 'x' singleton followed by a tag comprised of up to 8 alphanumeric characters. **Example** • en-GB-x-boe (British English with labels modified as per Bank of England localisation)
FIRE report currency	Currency used within report for all monetary references	Text (short)	**Syntax** • Selected single currency from enumerated list of alphabetic codes as defined in ISO 4217[13] **Example** • USD

11 ISO (2002), ISO 639 Language code

12 ISO (2020), ISO 3166 Country codes

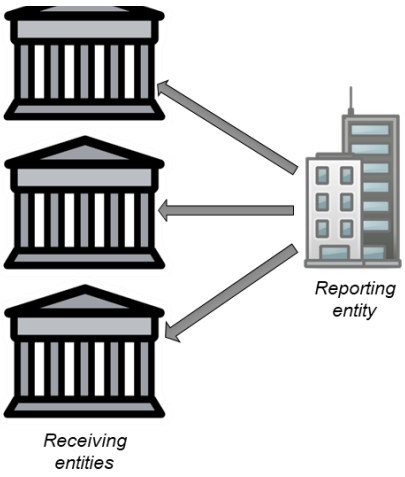
13 ISO (2015), ISO 4217 Currency codes

1. Institution-initiated reporting

Institution-initiated reporting represents the vast majority of incident reporting implementations. Although specifics vary, the underlying premise for institution-initiated reporting remains the same, i.e., an entity experiences an incident and elects to report it voluntarily or, depending on the circumstances, the incident triggers a reporting obligation to one or more receiving entities.

The nature of the information flows is **event-driven**, and **unidirectional** from reporting entity to receiving entities (as shown in **Figure 2**). Depending on individual reporting requirements of each receiving entity, more than one incident report may need to be issued for the same incident.

Figure 2: Institution-initiated reporting



The information requirements for institution-initiated reporting are grouped into four distinct collections (as shown in **Figure 3**), with the following characteristics:

- **Reporting Details**: *who issued the report, and to whom?*
- **Incident Details**: *what happened / is happening?*
- **Impact Assessment**: *what are the negative effects?*
- **Incident Closure**: *what caused the incident, and what remedial action(s) will be taken?*

Collectively, these information items provide receiving entities with the necessary information to understand incidents as they evolve and to act accordingly.

Figure 3: Breakdown of information item grouping for institution-initiated reporting

1.1 Reporting Details	1.2 Incident Details	1.3 Impact Assessment	1.4 Incident Closure
1.1.1 Reporting Entity	1.2.1 References	1.3.1 Severity Rating	1.4.1 Cause
1.1.2 Receiving Entity	1.2.2 Incident	1.3.2 Affected Parties	1.4.2 Lessons
1.1.3 Contact Details	1.2.3 Change(s) since Previous Report	1.3.3 Services and Resources	1.4.3 Supplemental Documentation
	1.2.4 Date / Time Markers	1.3.4 Impact	

1.1. Reporting Details

The information items associated with the reporting entity describe:

(i) attributes related to the reporting entity;

(ii) details of which receiving entities should be in receipt of this report instance; and

(iii) contact information for individuals at the reporting entity whom receiving entities may contact regarding the incident, if required.

1.1.1. Reporting Entity

These information items contain basic referencing and classification fields for the reporting entity. Apart from the **entity name** and **ultimate parent name**, which reflect the entity's legal or most commonly used designation (and that of its parent), the remaining items are structured to support analysis across the reporting entity data set by receiving entities.

Two information items are defined with respect to unique entity identifiers:

- **global identifier(s)**: where reporting information may be shared across recipients, global recognised identification schemes such as LEI codes (as defined in ISO 17442-1:2020[14]) provide a mechanism to reconcile reports for the same entity irrespective of where FIRE is implemented. However, as use of any given global identification scheme may not be universal, flexibility needs to be provided both in terms of discretion to implement, and in how the information item may be populated by reporting entities.
- **local identifier(s)**: In some jurisdictions and supranational structures, pre-existing identification schemes are already in use to uniquely identify reporting entities. The reporting entity would include the name of the scheme(s) and corresponding identifier(s) as defined by the relevant receiving entities.

Information Item	Purpose / Description	Field Type	Additional Syntax & Validation Rules, and Example Data
entity name	Name of entity that has submitted the report (e.g. formal legal name or most commonly used designation)	Text (short)	**Example** (fictitious) • *Megabank Inc.*

global identifier(s)	Unique and globally consistent identifier for each entity	Array (key-value)	**Syntax**
			• Array of (one or more) Text (short) pairs in the form [name of identifier, value of identifier]
			Validation
			• If "LEI" identifier is used, enforce validation rules for unique 20 alphanumeric character code in line with ISO 17442-1:2020
			  ○ Numbers 1-4 always show the ID of the LOU that issued the LEI.
			  ○ Numbers 5-6 always have a value of 0.

[14] ISO (2020), *ISO 17442-1:2020 - Financial services – Legal Entity identifier (LEI) – Part 1: Assignment*.

Information Item	Purpose / Description	Field Type	Additional Syntax & Validation Rules, and Example Data
			○ Numbers/Letters 7-18 are unique to each entity. ○ Numbers 19-20 are for verification purposes. • If "" (blank / no identifier), free text allowed **Examples** (fictitious) • *LEI, 123400ABC123DEF45699* • *, <free text>*
local identifier(s)	Unique identifier(s) for the reporting entity used locally within the jurisdiction of the receiving entity	Array (key-value)	**Syntax** • Array of (one or more) Text (short) pairs in the form [name of identifier, value of identifier] **Validation** • If "" (blank / no identifier), free text allowed **Example** (fictitious) • *FRN, 1234567* • *ABI, 11111* • *, <free text>*
ultimate parent name	Name of the ultimate parent undertaking of the group to which the reporting entity belongs, where applicable	Text (short)	**Example** (fictitious) • *MegaGroup*

Entity Type

To support the ability to examine a subset of reporting data based on the nature of the reporting entity, an information item capturing **entity type** has been included with the format. In terms of design, although a variety of existing industry classification schemes were considered as potential reference points to support enumeration (e.g. ISIC, NAICS), none were judged to be suitable matches. In addition, many jurisdictions already have entity type definitions codified within local laws and regulations, with uses spanning well beyond incident reporting.

Therefore, the approach taken for entity type is similar to entity identifiers, with full discretion provided on the schema used, and the relevant enumeration(s) selected from that schema. This method supports the use of multiple schemas in line with individual implementer needs and offers both backwards and forwards compatibility with existing and future schemas.

Information Item	Purpose / Description	Field Type	Additional Syntax & Validation Rules, and Example Data
entity type(s)	Specifies type of entity in accordance with chosen schema(s)	Array (key-value)	**Syntax** • Array of (one or more) Text (short) pairs in the form [name of schema, selected enumeration] **Validation** • If "" (blank / no schema), free text allowed

Information Item	Purpose / Description	Field Type	Additional Syntax & Validation Rules, and Example Data
			Example (fictitious) • *Schema1, EntityType1* • *Schema2, EntityTypeA*

Country of Entity

To support incident reporting to receiving entities across jurisdictions, the domicile of the reporting entity is captured using the **entity country** information item (affected locations are captured separately under *impact geographic spread*). To underpin this item, the ISO 3166 Country Codes standard is leveraged, specifically the widely-used **alpha-2** two-letter country codes (e.g., internet country code top-level domains). This option has the benefit of brevity, and optimised encoding length, but may not be immediately discernible by a human reader.

Information Item	Purpose / Description	Field Type	Additional Syntax & Validation Rules, and Example Data
entity country	Country in which reporting entity is domiciled	Enumerated	**Syntax** • Text (short) based enumerated list country codes using on ISO 3166 alpha-2 encoding **Example** • *ES*

1.1.2. Receiving Entity

This section is designed to enable several scenarios related to the delivery and routing of incident reports:

- The **recipient identifier(s)** information item enables the reporting entity to send the same incident report to multiple receiving entities simultaneously, thereby driving one-to-many efficiencies. This item can also support cross-authority arrangements that centralise receipt of incident reports, for onward distribution. However, this process requires that all receiving authorities are at the same stage in the incident reporting lifecycle (see *incident status* in Section 1.2.2). Upon receipt, the receiving entities would be aware of all other entities that had also received the same incident report from the reporting entity.

- The **recipient history** information item is used to show the entities that have previously received reports regarding the same incident, but not the current incident report instance being issued. This item could be used to send an initial incident report to an additional receiving entity whose reporting trigger comes into effect later in the incident lifecycle.

- The **onward forwarding** information items are not exposed to reporting entities. Instead, the items provide a facility for a receiving entity to forward an incident report to other entities who have not been informed of the incident directly (assuming appropriate information sharing arrangements are in place).

Example

	Scenario steps	Receiving Entity information items
1	An initial incident report is sent to authority AAA.	recipient identifier(s): AAA
2	The initial incident report is subsequently communicated to authority BBB by the reporting entity.	recipient identifier(s): BBB recipient history: AAA
3	Both authority AAA and BBB receive the same intermediate report concurrently from the reporting entity.	recipient identifier(s): AAA, BBB recipient history: AAA, BBB
4	Authority AAA has an information sharing arrangement with authority CCC and forwards the intermediate report from Step 3. CCC knows that they are receiving this report from AAA and not from the reporting entity, as they are not listed in recipient identifier(s) information item.	recipient identifier(s): AAA, BBB recipient history: AAA, BBB forwarding sender: AAA forwarding recipient(s): CCC

If a receiving entity receives a report where they are not referenced in either the recipient identifier(s) or forwarding recipient(s), then this report instance was not intended for them. In such circumstances, the receiving entity should delete the information received, and notify the originator that this report has been sent wrongly addressed. However, the reporting entity and any forwarding sender should implement appropriate controls to prevent accidental data loss from incorrect recipient addressing. Where numerous reporting obligations exist that may trigger independently, the sequencing of incident reports throughout the incident lifecycle is determined by the relative date/time stamp of each report (see section 1.2.4).

To uniquely reference receiving and forwarding entities within these information items, the use of LEI codes is supported, though other schemes and free text can also be used.

If implementing the discretionary incident forwarding feature, the receiving entity should first determine the circumstances under which use of the forwarding feature would be triggered in line with their own incident reporting objectives, as well as the extent to which information reported directly on incidents can be shared without conflicting with any other obligations. The receiving entity should also ensure that appropriate information sharing arrangements are in place to safeguard the transfer of incident reporting information between parties, and that forwarding recipient(s) have measures in place to handle such information on a 'need to know' basis (including, but not restricted to, MoU clauses, technical controls, access controls, personnel vetting, etc…). Finally, the receiving entity should put mechanisms in place to notify the originating reporting entity when forwarding takes place based on their regulatory and supervisory practice.

Information Item	Purpose / Description	Field Type	Additional Syntax & Validation Rules, and Example Data
recipient identifier(s)	Specifies the identifier(s) for the receiving entity(ies) to which this report is addressed as selected by the reporting entity	Array (key-value)	**Syntax** • Array of (one or more) Text (short) pairs in the form [name of identifier, value of identifier] **Validation** • If "LEI" identifier is used, enforce validation rules in line with ISO 17442-1:2020 • If "" (blank / no identifier), free text allowed

Information Item	Purpose / Description	Field Type	Additional Syntax & Validation Rules, and Example Data
			Example (fictitious) • *LEI, 123400ABC123DEF45699* • *, Authority X*
recipient history	Specifies the identifier(s) for the receiving entity(ies) to which previous reports for the same incident have been sent by the reporting entity	Array (key-value)	**Syntax** • Array of (one or more) Text (short) pairs in the form [name of identifier, value of identifier] **Validation** • If "LEI" identifier is used, enforce validation rules in line with ISO 17442-1:2020 • If "" (blank / no identifier), free text allowed **Example** (fictitious) • *LEI, 123400ABC123DEF45699* • *, Authority X*
forwarding sender *(not collected)*	Specifies the identifier for the report recipient that is performing the onward sharing of an incident report	Array (key-value)	**Syntax** • Array of (one or more) Text (short) pairs in the form [name of identifier, value of identifier] **Validation** • If "LEI" identifier is used, enforce validation rules in line with ISO 17442-1:2020 • If "" (blank / no identifier), free text allowed **Example** (fictitious) • *LEI, 123400ABC123DEF45699* • *, Authority X*
forwarding recipient(s) *(not collected)*	Specifies the identifier for the receiving entity(ies) to which this report is forwarded by a report recipient	Array (key-value)	**Syntax** • Array of (one or more) Text (short) pairs in the form [name of identifier, value of identifier] **Validation** • If "LEI" identifier is used, enforce validation rules in line with ISO 17442-1:2020 • If "" (blank / no identifier), free text allowed **Example** (fictitious) • *LEI, 123400ABC123DEF45699* • *, Authority X*

1.1.3. Contact Details

In case the receiving entity requires further information from the reporting entity following the submission of an incident report, the reporting entity is requested to designate at least one primary representative to act as a point of contact. As the use of single or multiple contacts varies across existing incident reporting arrangements, the **entity contact** information item has been designed to support one or more contacts, with the ability for the receiving entity to implement in line with their local needs. Contact email and phone numbers are both deemed required information items, so as to have two forms of communication channels to reach the entity representative.

Information Item	Purpose / Description	Field Type	Additional Syntax & Validation Rules, and Example Data
entity contact(s)	Name and contact information for one or more entity representatives in relation to the incident being reported	Container	**Syntax** • Wrapper for each entity contact instance **Validation** • Must have at least one contact entry where contact type = "Primary"

contact type	Denotes primary versus alternate contact preference for each contact	Enumerated	**Syntax**
			• Text (short) enumerated list with the following values:
			  ○ Primary
			  ○ Alternate
			Example
			• *Primary*

contact name	Name and surname of the contact person of the reporting entity	Text (short)	**Example** (fictitious) • *John Smith*
contact email	Email address of the contact person of the reporting entity	Text (email)	**Example** (fictitious) • *john.smith@email.com*
contact phone	Telephone number (including country code) of the contact person of the reporting entity	Text (telephone)	**Example** (fictitious) • *+11234567890*
contact role	Job role of the contact person of the reporting entity	Text (short)	**Example** (fictitious) • *Senior Officer*
contact department	Department title of the contact person of the reporting entity	Text (short)	**Example** (fictitious) • *Regulatory Liaison Team*
contact recipient	Recipient(s) for which entity contact is appropriate	Array (list)	**Syntax** • Populated dynamically using populated list of **recipient identifier(s)** **Validation** • Must be one or more entries on recipient identifier list, if selected. If blank, contact is valid for all recipients. **Example** (fictitious) • *Authority X*

1.2. Incident Details

The information items associated with the incident being reported describe:

(i) reporting entity generated unique identifiers for the incident or others that may be related;

(ii) the nature and circumstances of the incident, which are augmented and refined as the incident evolves;

(iii) actions taken or reactions to the incident that have transpired since the previous incident report; and

(iv) timing information for key incident milestones.

1.2.1. References

To support the tracking of individual incidents, and possible relationships between them, the format uses two identifying reference fields which serve different purposes:

- The **entity internal incident ID** information item captures the unique identifier that the reporting entity uses internally within its organisation to refer to the incident. Receiving entities would use this item to identify and collate all reports associated with the same incident.
- The **entity related incident ID(s)** information item provides the reporting entity with the ability to associate this incident to previous incidents that the entity has experienced (whether previously reported or not) using their internal referencing scheme. Receiving entities would thereby have access to the same relational information as the reporting entities.

When combined with onward forwarding between receiving entities, the entity provided IDs act as the unique key across recipients when engaging with the reporting entity on an individual or collective basis.

Information Item	Purpose / Description	Field Type	Additional Syntax & Validation Rules, and Example Data
entity internal incident ID	Unique reference code issued by the reporting entity unequivocally identifying the incident	Text (short)	**Example** (fictitious) • *INC123456789*
entity related incident ID(s)	Reporting entity can create a relationship to other current or previously resolved	Array (list)	**Syntax** • Array of Text (Short) **Validation** • Can have zero, one or more entries **Example** (fictitious)

Information Item	Purpose / Description	Field Type	Additional Syntax & Validation Rules, and Example Data
	incident(s) that may be relevant		• *INC1111111111* • *INC2222222222* • *INC3333333333*

1.2.2. Incident

This section describes the base attributes of the incident and captures what occurred. As with other elements of incident information, there are competing requirements that need to be addressed:

- driving **greater consistency** through maximal use of pre-defined structured information items, such as to promote common interpretation, expression, processing and analysis of incident reporting information; whilst
- **maintaining flexibility** and the ability to record qualitative details of incidents that cannot be easily reflected through pre-canned options, especially when it is not possible to account for all possible permutations or situations.

Report phase and incident status

Before describing the incident, the phase for which the report is being generated needs to be determined based on the receiving entity's incident reporting trigger criteria, as well as the status of the incident, and whether previous reports have been issued.

The format adopts a three-stage workflow reflected in the **report phase** information item, which reflects the most common approach in current use by authorities (albeit using different terminology), as reflected in the FSB's work on Cyber Incident Reporting[15]:

- **initial**: the first incident report issued to one or more receiving entities, based on the recipients' reporting trigger criteria.
- **intermediate**: additional reports that may be issued by the reporting entity in regard to the same incident based on further recipient reporting trigger criteria until and including when the incident is resolved.
- **final**: concluding report(s) supplied in line with receiving entity expectations, which contains relevant post-incident findings and remedial actions.

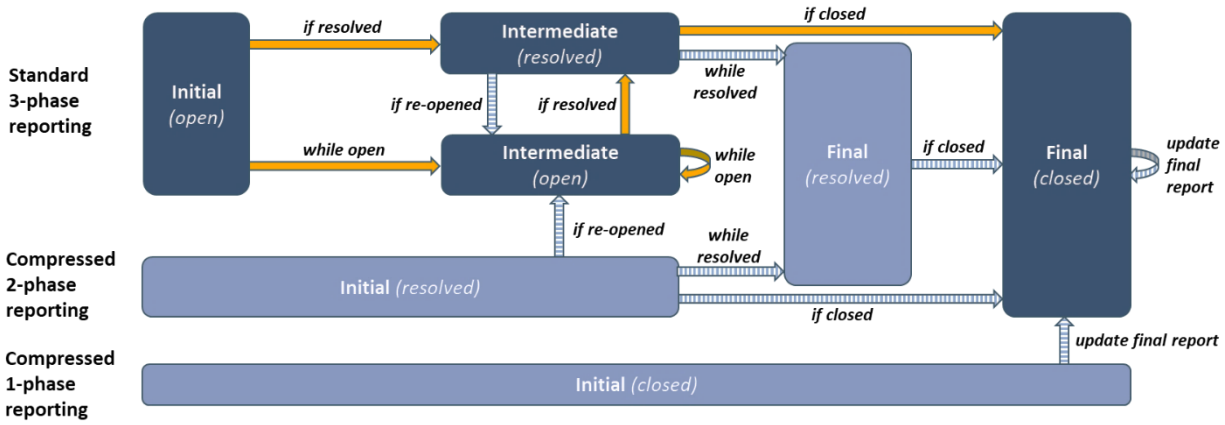
Figure 4 illustrates the transition between states and the interplay with the **incident status** information item.

[15] FSB (2023b)

In most cases, when triggered, the incident reporting workflow will pass through these three stages in sequence, with the potential for multiple intermediate or final reports to be issued. However, there are permitted edge case combinations:

- **initial / resolved**: where the criteria for an Initial report are met but the incident has already been resolved (compressed 2-phase reporting). Given the *resolved* state, the data requirements as set out under the Intermediate phase would apply.
- **initial / closed**: where the criteria for an Initial report are met but the incident has already been closed (compressed 1-phase reporting). Given the *closed* state, the data requirements as set out under the Final phase would apply.
- **final / resolved**: where the trigger for final reporting occurs prior to the conclusion of the post-incident review, and where an initial position on information items associated with incident closure is required. This use case also implies that multiple final reports may be submitted to augment or adjust previously issued reports.

Figure 4: Report phase workflow and valid states



LEGEND	
Report	*Most common workflow states*
→	*Most common state transitions*
Report	*Rare but permissible workflow states*
⇢	*Rare but permissible state transitions*

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

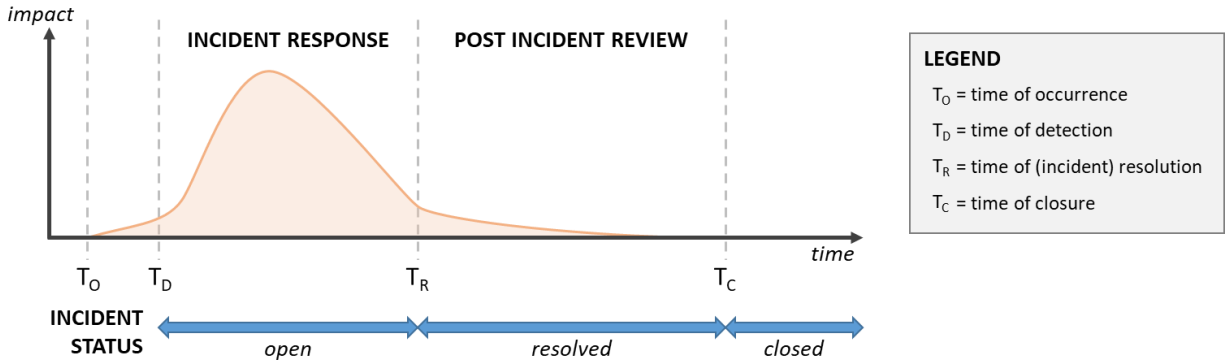
The status of an incident has been simplified down to three possible states, which are defined relative to key incident time markers (as shown in **Figure 5**):

- **open**: the period between the time of detection (T_D) and time of resolution (T_R), when the reporting entity is focused on responding to the incident, bringing impacts under control, and returning to a steady, though possibly not normal, state.
- **resolved**: the period between the time of resolution (T_R) and time of closure (T_C), when the immediate negative effects of the incident have been addressed, though longer-

term impacts may take longer to recover from. A formal post-incident review is typically undertaken during this period.

- **closed**: the state assumed when the post-incident review has been concluded (T_C), with findings and any remedial activities identified.

Figure 5. Incident status relative to lifecycle state transitions



It is important to note that the transition between incident states is intended to be unidirectional in nature in most circumstances, i.e. *open* from *resolved*, or *resolved* from *closed*. However, there may be rare occasions where an incident initially deemed as resolved is determined to still be on-going, and therefore may require the ability to revert to an *open* state to avoid the additional burden of initiating a new incident reporting workflow. A separate but repeat occurrence of an incident is expected to be treated as a new incident and initiate a new workflow, with the previous occurrence of the incident referenced using the related incident ID.

In institution-initiated reporting, the status of the incident also drives another significant feature of the format referred to as **reporting phase optionality**. At the outset of an incident, there are two key early assessment challenges that need to be considered:

- **information confidence**: in early stages, it may not be possible to determine the underlying nature of an incident when situational awareness is low.
- **undue initial burden**: the priority for the reporting entity is to respond to the incident and bring its effects under control. Excessive reporting requirements during this period may distract or impede the reporting entity from achieving this outcome.

Therefore, the scale of required reporting information at the outset needs to be as minimal as possible, but sufficient to meet the requirements of the receiving entity to execute its mandate. As the incident progresses through to closure, the format adjusts the reporting phase optionality to reflect information that would be expected at each transition point (see Annex B for breakdown of all institution-initiated reporting information items and their optionality). Note that the format reflects a minimum set of information for reporting phase optionality, and that receiving entities may additionally require the collection of any optional information item to reflect their local needs.

Information Item	Purpose / Description	Field Type	Additional Syntax & Validation Rules, and Example Data

report phase	Describes the phase of the incident for which the report has been issued	Enumerated	**Syntax**
			• Text (short) list with one of the following values:
			  ○ Initial
			  ○ Intermediate
			  ○ Final
			Example
			• *Initial*

incident status	Represents the incident lifecycle in three stages	Enumerated	**Syntax**
			• Text (short) list with one of the following values:
			  ○ Open
			  ○ Resolved
			  ○ Closed
			Validation
			• Reject incompatible combinations with report phase:
			  ○ Intermediate + Closed
			  ○ Final + Open
			Example
			• *Open*

Incident title and description

Two important qualitative information items that provide an overall reflection of the incident at different levels of granularity are incident title and incident description. They serve different purposes:

- the **incident title** information item is intended to be a concise reflection of the incident, accessible and interpretable by a broad (and possibly non-technical) audience. A useful analogy for these information items is that *incident title* represents the mainstream media headline while *incident description* contains the underlying story, with the aim to be sufficiently distinctive to differentiate between incidents. The incident title may vary across reports for the same incident to more accurately reflect the nature of the incident as it evolves (as the reference identifiers maintain tracking through incident lifecycle), as it may not be possible to provide such specificity at the outset of the incident.

- the **incident description** information item enables the reporting entity to provide a more extensive qualitative description of the incident, without imposing additional constraints. As with the title, the description content can evolve over time to reflect the current understanding of the incident. The item can also be used as a catch-all for idiosyncratic receiving authority reporting requirements that are not reflected in other incident-related information items within the format. It should be noted that actions taken or planned by the reporting entity are captured separately.

Information Item	Purpose / Description	Field Type	Additional Syntax & Validation Rules, and Example Data
incident title	Incident name or headline described by reporting entity	Text (short)	**Example** (fictitious) • *Intermittent Access to Online Banking Platform*
incident description	Summary description of the most relevant aspects of the incident to supplement structured information items	Text (long)	**Example** (fictitious) • *Extended description of reported incident*

Incident type

One of the most common methods used by receiving authorities to categorise incidents is based on type. However, although the use of this data field is near-universal, its implementation across authorities is typically bespoke. With an objective of greater convergence, this specification seeks to address this source of fragmentation by proposing a consistent approach to **incident type** classification.

When comparing existing incident reporting practices, the assignment of incident type often resulted in a **conflation between the event and its causation**. For example, an existing categorisation of incident type might include “social engineering” or “phishing”, but these types describe the method or vector rather than the operational event that took place (e.g. a data breach). It would be more accurate to capture those elements when describing the underlying cause(s) of the incident.

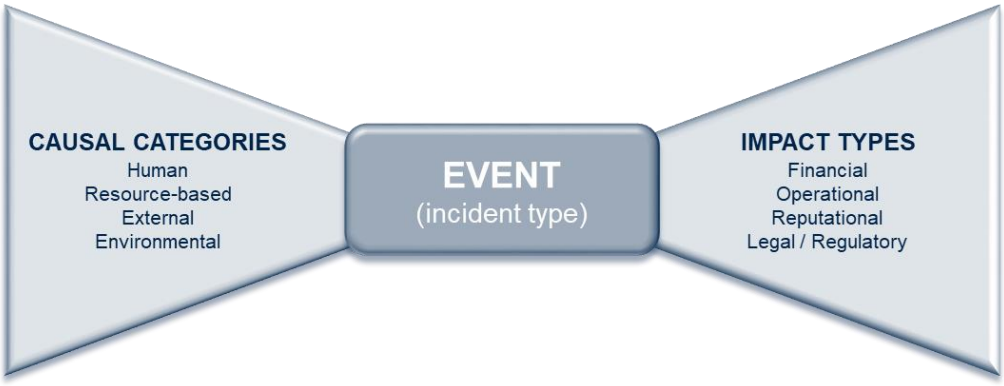
To account for this issue, the design within FIRE delineates between *causation* (in Incident Closure pillar), *incident type*, and the resultant *impacts* (within Impact Assessment pillar), based on the Bow-Tie Method[16] (**Figure 6**). The incident type enumerations found in Annex C are **cause-agnostic** and can arise from a range of possible threats or hazards. This approach[17] allows for a more concise and consistent categorisation of incidents, whereas the possible causes can be more extensive and elaborate in nature.

---

16 The Bow-Tie Method is a risk assessment method that can be used to analyse and communicate risk scenarios, taking its name from the shape of the diagram which resembles a bowtie, and whose conception is generally attributed to David Gill, engineer at ICI in the 1970s.

17 This approach mirrors and adapts a similar method proposed for event types found in:
Federal Reserve Bank of Richmond (2020), Curti et al., *Cyber Risk Definition and Classification for Financial Risk Management*

Figure 6. Application of Bow-Tie Method within specification



In some cases, the underlying cause(s) of an incident **may not be fully understood** until the later stages of an incident or possibly not until a post-incident review is performed. It is therefore beneficial to have cause/event separation in the early stages of reporting. It is also possible for more than one incident type to be applicable depending on the circumstance, e.g. the deployment of malware coupled with data exfiltration.

Information Item	Purpose / Description	Field Type	Additional Syntax & Validation Rules, and Example Data
incident type	Provides categorisation of incident based on event type (not causation)	Array (list)	**Syntax** • Array of enumerated Text (short) types • Multiple selection from list set out in Annex C **Validation** • Can have more than one incident type • Incident type may not be fully known at the outset, but becomes 'essential' when incident is resolved **Example** • *Data Breach*

Incident artefact(s)

While responding to an incident, a reporting entity may uncover information that could inform causation and/or incident origin and may be of relevance to receiving entities. The incident artefact information item provides a flexible mechanism to optionally report such information through use an unstructured long text data type. The type of artefacts for which this information item could be used include, but are not limited to: IP addresses, URL addresses, domains, file hashes, malware data, network activity data, e-mail message data, DNS requests and registry configurations, user account activities, or database traffic.

Information Item	Purpose / Description	Field Type	Additional Syntax & Validation Rules, and Example Data
incident artefact(s)	Facility to include specific details that may inform incident causation	Text (long)	**Example** • *IP addresses, 1.1.1.1* • *Domains, example.com*

Incident discovery method

The **discovery method** associated with each incident represents a useful attribute, both for the reporting and receiving entities. This data point can provide insight into the different routes through which entities becomes aware of incidents, which can inform future incident detection capability development. List options have been based on an adjusted version of a similar list provided in VERIS[18], with some additional and consolidated entries. As it may not be possible to account for every possible discovery method, an '*other*' option is included to allow for supplemental method detail to be reflected using the incident description information item.

Information Item	Purpose / Description	Field Type	Additional Syntax & Validation Rules, and Example Data
incident discovery method	Indication of how the incident has been discovered by the reporting entity	Enumerated	**Syntax** • Text (short) list with single selection from Annex D **Example** • *External – Law Enforcement*

Incident reporting trigger

As **reporting trigger** criteria are uniquely defined by each receiving entity, the underlying reasons why a reporting entity would issue an incident report will vary greatly. Therefore, this information item has been generalised to reflect the impact types (as per Section 1.3.4) or actions taken that may trigger a reporting obligation.

To account for all possible scenarios, the reporting entity can either indicate which trigger criteria applied (for each receiving entity using previously identified recipient identifiers) or note that reporting is not trigger-related. An additional option is provided to support the use of occurrence or detection-driven reporting criteria.

- **operational**
- **financial**
- **reputational**
- **legal/regulatory**
- **external**
- **geographic spread**
- **incident type** (e.g. data loss)
- **level of internal escalation** (which may be reflected in the severity of the incident)

[18] Verizon (2019), *Vocabulary for Event Recording and Incident Sharing (VERIS)* (Discovery_method enumeration)

- **bodies notified** (other authorities/agencies notified)
- **time-based requirement** (i.e. reporting obligation within defined time period from specific time marker)
- **risk to objective(s)** (where the impact stemming from the incident may put at risk one or more receiving entity objectives)
- **not triggered** (proactively or retrospectively reported)
- **other**

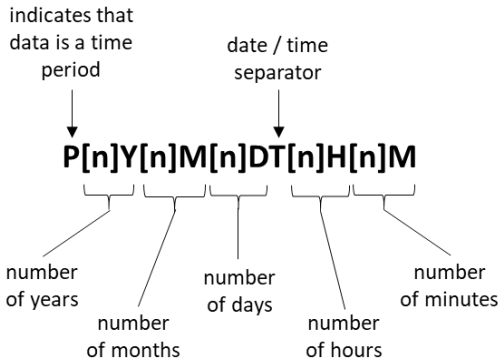
To support concurrent triggers across multiple receiving authorities, recipient identifiers are reflected against each of the relevant triggers.

Information Item	Purpose / Description	Field Type	Additional Syntax & Validation Rules, and Example Data

incident reporting trigger(s)	Provides ability for reporting entity to declare which aspect(s) of the reporting criteria have been triggered, and for which report recipient.	Array (list)	**Syntax**
			• Array of one or more triplets in the form: [Text (short) enumerated list, Text (short), Text (long)]
			• Enumerated list selection from following values:
			  ○ operational
			  ○ financial
			  ○ reputational
			  ○ legal/regulatory
			  ○ external
			  ○ geographic spread
			  ○ incident type
			  ○ level of internal escalation
			  ○ bodies notified
			  ○ time-based requirement
			  ○ risk to objective(s)
			  ○ not triggered
			  ○ other
			• Text (short) with value of *recipient identifier*
			• Optional Text (long) to provide further context
			Validation
			• Receiving entities selected from entries previously provided
			Example
			• *financial, Authority X, estimated financial loss exceeding $1m*

Estimated resolution timeframe

An information item for providing an **estimated timeframe for incident resolution** is included within the format such that the reporting entity can provide an indicative view to receiving entities of when they might expect the incident to be brought under control. The ISO 8601 standard[19] is used to record time periods in a consistent fashion. Each time element can be optionally expressed, allowing reporting entities to provide estimates in minutes, hours, days, months or even years.



By combining two information items, the design enables reporting of a time range, to avoid undue specificity when timeframe of resolution may not be precisely understood but could be approximated.

Information Item	Purpose / Description	Field Type	Additional Syntax & Validation Rules, and Example Data
estimated timeframe for resolution	Provides ability for entities to give indicative timeframe for incident resolution (at least or equal to a specified duration)	Duration	**Syntax** • As per ISO 8601 standard, subset of syntax can be provided **Examples** • *(At least or exactly) 3 hours and 30 minutes would be expressed as PT3H30M*
estimated timeframe for resolution max	Provides ability for entities to give indicative maximum timeframe for incident resolution	Duration	**Syntax** • As per ISO 8601 standard, subset of syntax can be provided. • Optional indication for maximum duration, to create a range when paired with previous information item **Examples** • *At most 6 hours would be expressed as PT6H*

1.2.3. Change(s) since Previous Report

Whereas the previous section on incident details seeks to capture the evolving nature of the incident, information items within this section have been grouped together to reflect new incident developments that have arisen in between reports (or as part of the initial report if applicable). The six information items in this section are a mix of structured and unstructured formats, based on where content can be standardised versus providing maximum flexibility. Receiving entities implementing the format may choose to provide additional guidance for specific content they wish to receive within free text fields.

[19] ISO (2019), *ISO 8601-1:2019 Date and time – Representations for information interchange – Part 1: Basic rules*

- **actions taken**: steps that the reporting entity has taken to bring the incident under control. Rather than pre-empt every conceivable form of action that could be taken, this information item is deliberately left as free text. The actions recorded are intended to be report-specific. However, a complete timeline of actions over the course of the incident can be reconstituted in the final report, by consolidating this information item's entries across all reports related to the same incident (alongside report timing information).

- **actions planned**: steps that the reporting entity plans to take to bring the incident under control (reporting entity can also indicate where no planned actions have been identified or are necessary).

- **public reaction**: summary of reporting, statements or sentiment arising from mainstream or social media channels.

- **communications issued**: indicating whether the reporting entity has issued or updated any external communications in response to the incident.

- **bodies notified**: aside from financial authorities that may be direct recipients on these incident reports, this information item captures the names of other authorities or agencies that have also been notified of the incident. These bodies could include relevant national competent authorities (e.g. cyber security agencies), law enforcement, or any interested stakeholder group (domestic or international) with an interest in the incident.

Information Item	Purpose / Description	Field Type	Additional Syntax & Validation Rules, and Example Data
actions taken	Description of actions taken by reporting entity to bring incident under control	Text (long)	**Example** (fictitious) • *Entity took this step to resolve incident*
actions planned	Description of actions planned by reporting entity to bring incident under control	Text (long)	**Example** (fictitious) • *Entity plans to take the following actions to resolve incident*
public reaction	Description of the current level of media or public discourse resulting from the incident	Text (long)	**Example** (fictitious) • *Incident has received the following level of media attention, and presence on social media*
comms issues	Description of the communication about the incident to external stakeholders	Text (long)	**Example** (fictitious) • *Entity has issued the following formal communications regarding this incident*
bodies notified	List of all non-financial authorities or relevant agencies	Array (list)	**Syntax** • Array of Text (short) **Validation**

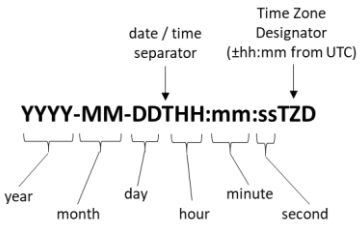
Information Item	Purpose / Description	Field Type	Additional Syntax & Validation Rules, and Example Data
	(domestic and international) that have been notified of incident		• Can have zero, one, or more entries **Example** (fictitious) • *National cyber agency* • *Law enforcement*

1.2.4. Date / Time Markers

Incident information often contains date / time markers that reflect the specific timing of milestones within an incident. Four of these markers have already been referenced in **Figure 5**, and are supplemented by two further markers:

- **report time**: records when a specific report was issued. The receiving entity needs this information to determine the sequencing of reports related to the same incident.
- **time of next report**: an estimate provided by the reporting entity to manage expectations for when the next report is expected to be issued. This will to some extent depend on the reporting triggers for intermediate reports defined by the receiving entity, e.g. a fixed time period between reports, intermediate reporting based on a change in circumstances, or intermediate reporting that is only required upon incident resolution.

As with the handling of time periods in Section 1.2.2, the syntax for date / time markers also uses the ISO 8601:2019 standard, with two notes in relation to time:



- the inclusion of **seconds**, in case precision is required;
- **Time Zone Designator (TZD)** allows for encoding of timing information to be captured using local time zone and subsequently shifted relative to UTC (Universal Time Coordinated).

Information Item	Purpose / Description	Field Type	Additional Syntax & Validation Rules, and Example Data
time of report	Date and time at which the report is issued	Datetime	**Validation** • Date/time must be in the past. **Example** • *2024-06-15T12:32:20+00:00*
time of occurrence	Date and time at which the incident has occurred (if known)	Datetime	**Validation** • Date/time must be in the past. • Must be earlier than time of detection, resolution and closure **Example** • *2024-06-15T12:32:20+00:00*
time of detection	Date and time at which the incident was detected	Datetime	**Validation** • Date/time must be in the past.

Information Item	Purpose / Description	Field Type	Additional Syntax & Validation Rules, and Example Data
			• Must be later than time of occurrence (if provided) • Must be earlier than time of closure **Example** • *2024-06-15T12:32:20+00:00*
time of resolution	Date and time when services, activities and/or operations have been restored from the incident	Datetime	**Validation** • Date/time must be in the past. • Must be later than time of occurrence (if provided) • Must be earlier than time of closure **Example** • *2024-06-15T12:32:20+00:00*
time of closure	Date and time when the incident was closed and cause(s) identified	Datetime	**Validation** • Date/time must be in the past. • Must be later than time of detection and resolution **Example** • *2024-06-15T12:32:20+00:00*
time of next update	Date and time when the reporting entity expects to issue the next report	Datetime	**Validation** • Date/time must be in the future. **Example** • *2024-06-15T12:32:20+00:00*

1.3. Impact Assessment

Consequences arising from incidents are typically expressed in the form of impact, which is defined by ISO[20] 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, must be grounded in what is known or readily observable. For reporting entities, awareness of impacts is typically limited to first-order effects either experienced within the reporting entity or emanating to its immediate community of stakeholders. Consequently, the scope of impact information from individual reporting entities is constrained by the entity's knowledge of downstream impacts, and possible contagion ramifications for the rest of the financial system and the wider economy. In the case of sector-wide or cross-border incidents affecting many regulated institutions, financial authorities may wish to instigate authority-initiated reporting to perform impact assessment over a targeted subset of market sector participants and/or carry out jurisdiction-level evaluations.

Hence, the information items related to impact are grouped and ordered to reflect the sequence by which reporting entities might assess them:

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

- the categorisation of **severity** by the reporting entity;
- the **parties affected** by the incident;
- the entity **services and resources** affected by the incident; and
- a qualitative expression of **impact** using normalised scales.

1.3.1. Severity Rating

Whereas impact assessment seeks to evaluate the consequences of an incident with an outward focus, the notion of **severity** provides an indication of the significance and urgency that the reporting entity places on addressing the incident. The approaches to severity used by institutions and authorities are typically tailored and therefore idiosyncratic to each organisation.

This presents a dilemma with two opposing drivers:

- achieving greater convergence to enable cross-entity comparability; whilst
- respecting individual institutional choices and diversity across the ecosystem.

To strike an appropriate balance, the two information items within this format related to severity are implemented as follows:

- the **entity severity** information item captures how the reporting entity internally references the severity of the incident in its own terms. The severity level can vary throughout the course of an incident. The level recorded in the final report is expected to represent *the most severe rating* assigned by the reporting entity over the course of the lifecycle of the incident.
- the **standardised severity** information item reflects a normalised interpretation of the reporting entity's severity as assessed against a common reference scale. By implementing a consistent scalar, it is possible to perform relative severity comparisons across the reported incident data set. As per the previous information item, the standardised severity reported in the final report reflects *the most severe rating* assigned by the receiving entity throughout the incident.

This approach seeks to promote a degree of normalisation, without forcing homogeneity across reporting entities. As the assignment of severity is performed by reporting entities from the point of incident detection and initiation of incident management procedures, standardised severity is an essential item across all institution-initiated incident reports. The standardised severity also incorporates the concepts associated with internal escalation depending upon the severity of the incident.

Information Item	Purpose / Description	Field Type	Additional Syntax & Validation Rules, and Example Data
entity severity	Describes the reporting entity's severity rating, as per their internal	Text (short)	**Example** (fictitious) • *Severity 2*

Information Item	Purpose / Description	Field Type	Additional Syntax & Validation Rules, and Example Data
	incident categorisation		

standardised severity	A standardised view of severity linked to observed impacts, to promote a consistent categorisation of severity across reported incidents	Enumerated	**Syntax**
			• Text (short) enumerated list with the following values (see Annex E for details):
			  ○ Nil
			  ○ Negligible
			  ○ Low
			  ○ Medium
			  ○ High
			  ○ Extreme
			Example
			• *Medium*

1.3.2. Affected Parties

To convey the extent to which other parties either within or beyond the finance sector may be affected by a reported incident, an information item describing the types of **affected parties** is included within the format, with the following options:

- **reporting entity**: the entity that has issued the report is directly affected by the incident (note that it is possible for the reporting entity to fulfil the reporting obligation on behalf of another entity in the same organisation, but not be affected).
- **other related entities**: other affected entities within the same organisation
- **business counterparties**: separate financial institutions where a pre-existing relationship is in place
- **other financial market participants**: other financial institutions affected by the incident not accounted for in the previous options
- **third-party vendors or service providers**: non-financial entities that support the financial sector
- **non-financial sectors**: affected entities outside of the financial sector
- **customers/consumers**: affected individuals or corporate clients who consume financial services from the reporting entity (or any affiliated entities)
- **vulnerable customers/consumers**: a subset of the previous option, describing individuals who, due to their personal circumstances, are especially susceptible to harm
- **general public**: people in society with no relationship to the reporting entity or its affiliates

Other parties may be affected by the same incident in two ways:

(i) as a direct or indirect consequence of the services affected at the reporting entity; or

(ii) because the same incident is affecting other entities in addition to the reporting entity.

A third information item for additional notes is included to provide supplemental context on the circumstances by which these parties were affected.

Information Item	Purpose / Description	Field Type	Additional Syntax & Validation Rules, and Example Data

affected parties	Describes the types of parties that have either been directly affected by the service disruption from the reporting entity, or as a result of the same incident but not via the reporting entity	Array (list)	**Syntax**
			• Array of Text (short) enumerated types, selected from:
			  ○ Reporting entity
			  ○ Other related entities
			  ○ Business counterparties
			  ○ Other financial market participants
			  ○ Third-party vendors or service providers
			  ○ Non-financial sectors
			  ○ Customers/consumers
			  ○ Vulnerable customers/consumers
			  ○ General public
			Validation
			• Can have multiple types of parties affected by the same incident
			Example
			• *Reporting entity*
			• *Other related entities*
			• *Other financial market participants*
			• *Customers/consumers*

related affected entities	List of all entities affected by the incident that are related to the reporting entity	Array (key-value)	**Syntax** • Array of (one or more) Text (short) pairs in the form [name of identifier, value of identifier] **Validation** • If "LEI" identifier is used, enforce validation rules in line with ISO 17442-1:2020 • If "" (blank / no identifier), free text allowed **Example** (fictitious) • *LEI, 123400ABC123DEF45699* • *, <free text>*
affected notes	Provides more extensive description of parties affected	Text (long)	**Example** (fictitious) • *Market-wide incident affecting multiple retail banks and their customer base*

1.3.3. 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. This information forms the next grouping of information items that can build towards an overarching impact assessment.

Services

The use of the term "service" in this format is intended to be synonymous with "operation", in line with the definition in the Joint Forum's 2006 high-level principles for business continuity[21]. However, as the focus of assessment is predominantly on externalised impacts, the preference for "service" is based on how external parties interact with the reporting entity, rather than affected operations within the reporting entity. The concept of service materiality is also decoupled and evaluated separately. This delineation allows for incidents involving internal services with no external impacts to be reported, if receiving entities opt to include such incidents within their reporting trigger criteria.

As multiple services may be disrupted during the same incident, the format is designed to capture nine attributes for each affected service, with the first four describing the nature of each affected service and disruption type:

- **service name**: the descriptive term used by the firm to identify the service.
- **service type**: in order to support the use of consistent classification of services affected, this information item provides a mechanism to map services against any chosen schemas (using the same method as entity type)
- **service critical**: as with severity, each reporting entity will have its own approach to defining levels of criticality for their services. Rather than implement a scalar, this information item contains a list of those receiving entities where the criteria for a critical or important service are met, as judged by the reporting entity.
- **service disruption type**: as services may be disrupted in a variety of ways, the format caters for a range of different disruption types as described in Annex F, which leverage the properties listed in the FSB Cyber Lexicon definition of "cyber security"[22] (also found in Annex I). The disruption types are firstly grouped in line with loss of these properties i.e. loss of availability, integrity, confidentiality, and also trust as an amalgam of the remaining properties. A second level of granularity is provided in the format to further differentiate between disruption types.

---

21 Basel Committee on Banking Supervision (2006), The Joint Forum, *High-level principles for business continuity*
The term "critical operation or service" is defined as *"any activity, function, process, or service, the loss of which would be material to the continued operation of the financial industry participant, financial authority, and/or financial system concerned. Whether a particular operation or service is "critical" depends on the nature of the relevant organisation or financial system."*

22 FSB (2018), *Cyber Lexicon*, November.
The term "cyber security" is defined as the *"preservation of confidentiality, integrity and availability of information and/or information systems through the cyber medium. In addition, other properties, such as authenticity, accountability, non-repudiation and reliability can also be involved."*

- **service downtime**: the duration of full or partial service unavailability is recorded in this information item. Where relevant based on the nature of the disruption, a set of two information items can be used to express a range, to allow for varying levels of precision or certainty.

Information Item	Purpose / Description	Field Type	Additional Syntax & Validation Rules, and Example Data
service(s) affected	Describes services provided by the reporting entity affected by the incident	Container	**Validation** • Possible to have incident with no services affected
service name	Descriptive term used by the reporting entity to identify the service	Text (short)	**Example** (fictitious) • *Push (Credit) Payments*
service type	Provides a method for the service to be categorised using one or more relevant schemas	Array (key-vale)	**Syntax** • Array of (one or more) Text (short) pairs in the form [name of schema, selected enumeration] **Validation** • If "" (blank / no schema), free text allowed **Example** (fictitious) • *Schema1, ServiceType1* • *Schema2, ServiceTypeA*
service critical	Captures a list of receiving entities where the service may be deemed as critical or important (in line with each recipient's definitions), as judged by the reporting entity	Array (list)	**Syntax** • Populated dynamically using populated list of **recipient identifier(s)** • If left blank, service is deemed to be non-critical with respect to all receiving entity regimes. **Example** (fictitious) • *Authority X*
service disruption type	Provides a method for consistent classification of different types of the service disruption	Array (list)	**Syntax** • Array of Text (short) enumerated types, selected from list set out in Annex F. **Validation** • Must have at least one type selected **Example** (fictitious) • *Availability Loss: Intermittent*
service downtime	(Minimum) time period from service being fully or partially unavailable to external end-users until regular activities or	Duration	**Syntax** • Used to express minimum or precise service downtime. • Null values represent zero downtime or not applicable. **Examples**

Information Item	Purpose / Description	Field Type	Additional Syntax & Validation Rules, and Example Data
	operations have been restored. (if applicable)		• *(At least) 4 hours would be expressed as PT4H*
service downtime max	Maximum estimated period of service disruption	Duration	**Syntax** • Optional maximum service down time used to express range when estimating. **Examples** • *At most 8 hours would be expressed as PT8H*

The subsequent information items, contained within each affected service, are used to provide a consistent expression of the scale of an incident, focusing on affected customer or consumer base, and transaction volume (where appropriate). This information can be qualitatively augmented using the supplemental **service/ resource notes** information item at the end of this section, for which receiving entities may issue guidance as part of local implementations.

Customer / Consumer Base

The majority of financial sector participant business models involve either B2B (business-to-business) or B2C (business-to-consumer) relationships. Although these relationships differentiate between customers (as purchasers of goods or services) and consumers (as end users of goods or services), this format combines these external parties as "external end users" of the reporting entity's services. The notion of "external end users" includes also other counterparties, as relevant, such as participants in a financial market infrastructure. Rather than describe the scale of user base affected per service involved, the format takes a simplified approach:

- **number of external end users affected**: reflects the total of customers and/or consumers affected by the incident.
- **percentage of external end users affected**: a percentage figure is also included so that the affected user base is considered in context of the typical total user base, as a pure number alone does not immediately convey a sense of scale.

Information Item	Purpose / Description	Field Type	Additional Syntax & Validation Rules, and Example Data
affected end user number	(Minimum) number of external end users (customers and/or consumers) affected for specific service	Integer	**Syntax** • Used to express minimum or precise number of external end users affected. **Validation** • Value must be non-negative number. **Example** • *(At least of equal to) 50000*
affected end user	Maximum number of external end	Integer	**Syntax** • Optional maximum number of external end users affected to express range when estimating.

Information Item	Purpose / Description	Field Type	Additional Syntax & Validation Rules, and Example Data
number max	users for specific service		**Validation** • Value must be non-negative number. **Example** • *(At most) 100000*
affected end user percentage	(Minimum) percentage of specific service's user base affected relative to total	Percentage	**Syntax** • Used to express minimum or precise percentage of service's user base that is affected. **Example** • *0.25 (at least or equal to 25%)*
Affected end user percentage max	Maximum percentage of specific service's user base affected relative to total	Percentage	**Syntax** • Optional maximum percentage of service's user base affected to express range when estimating. **Example** • *0.5 (at most 50%)*

Affected Transactions

To report on impacts to affected transaction flows associated with specific services, the reporting entity can indicate the number, percentage and/or value of transactions affected, depending on which information items have been implemented locally. In some cases, a sense of scale may be best conveyed using **transaction percentage** rather than through user counts. For example, a highly critical service may only have one downstream user (e.g. another regulated counterparty), but the user base metric would only reveal that 1 external end user was affected, which is not particularly informative in isolation. In different circumstances, knowledge of the **transaction number** or **transaction value** affected may also be critical to size the problem.

In addition, the **type of affected transaction** is optionally recorded using the Business Area groupings defined in Annex G, based on the ISO 20022 universal financial industry messaging scheme[23].

Information Item	Purpose / Description	Field Type	Additional Syntax & Validation Rules, and Example Data
affected transaction type	Types of transactions affected for a specific service, aligned to ISO20022 Business Areas	Array (list)	**Syntax** • Array of enumerated text (short) types, selected from list in Annex G **Example** • *Payments & Cash Management*
affected transaction number	(Minimum) Number of transactions	Integer	**Syntax** • Used to express minimum or precise number of transactions affected.

[23] ISO (2013), *ISO 20022 Universal Financial Industry Messaging Standard*

Information Item	Purpose / Description	Field Type	Additional Syntax & Validation Rules, and Example Data
	affected for a specific service		**Example** • *(At least or equal to) 50000*
affected transaction number max	Maximum number of transactions affected	Integer	**Syntax** • Optional maximum number of transactions affected to express range when estimating. **Example** • *(At most) 100000*
affected transaction percentage	(Minimum) percentage of transactions affected relative to typical total volumes for a specific service	Percentage	**Syntax** • Used to express minimum or precise percentage of transaction volume affected. **Example** • *0.6 (at least or equal to 60%)*
affected transaction percentage max	Maximum percentage of transactions affected	Percentage	**Syntax** • Optional maximum percentage of transaction volume affected to express range when estimating. **Example** • *0.8 (at most 80%)*
affected transaction value	(Minimum) value of transactions affected for a specific service	Decimal	**Syntax** • Used to express minimum or precise value of transactions affected. **Example** • *(At least or equal to) 1000000*
affected transaction value max	Maximum value of transactions affected	Decimal	**Syntax** • Optional maximum value of transactions affected to express range when estimating. **Example** • *(At most) 2000000*

Resources

The use of the term "resource" is intended to be a subset of the "asset" types defined in the FSB Cyber Lexicon[24], to align more closely to the concept of "supporting assets" defined in BCBS principles for operational resilience[25].

[24] FSB (2018).
The term "asset" is defined as *"something of either tangible or intangible value that is worth protecting, including people, information, infrastructure, finances and reputation."*

[25] Basel Committee on Banking Supervision (2021), *Principles for Operational Resilience*
The term "supporting assets" is defined as *"people, technology, information and facilities necessary for the delivery of critical operations."*

Incidents occur when the properties of resources are negatively affected, which can lead to disruption of the services which they support. For the purpose of incident reporting, the format takes a proportionate approach by defining the data structures to capture the **type(s) of resources** affected (Annex H), and their associated **properties** (Annex I).

However, capturing the scale or relative proportion of individual resources affected would be impractical to implement in a structured manner, and may only be fully understood and relevant following a post-incident review, which reveals the true extent of an incident. Instead, a **notes** information item for supplemental information associated with affected services or resources is included within the format. Receiving entities may issue guidance on content requirements for this item as part of local implementations.

Information Item	Purpose / Description	Field Type	Additional Syntax & Validation Rules, and Example Data
resource(s) affected	Describes the underlying resources affected in aggregate by the incident	Container	
resource type	Describes the types of underlying resources affected by the incident	Enumerated	**Syntax** • Text (short) enumerated list, with a single selection from Annex H **Example** • *Technology: ICT Hardware*
resource affected properties	Describes how the associated properties of each affected resource have been affected	Array (list)	**Syntax** • Array of Text (short) type entries, selected from enumeration from Annex I **Example** • *Availability*
service / resource notes	Provides more extensive description of services and/or resources affected	Text (long)	**Example** (fictitious) • *Irreparable network card hardware failure associated with payment processing system, causing intermittent re-routing of network traffic, and downstream impact to customer-facing transaction authorisation services*

1.3.4. 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 institutions to initially define and source accurate and timely data to use as part of incident response. Therefore, the format adopts a qualitative approach to evaluating impact, which can more easily be applied across all types of reporting entities.

This judgement-based method uses descriptive statements to define levels of increasing severity across a range of impact categories. Over the course of an incident, a reporting entity regularly performs 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 is therefore necessary to use a normalised set of impact scales, although the intent is not to supplant existing levels defined by either reporting or receiving entities. Instead, the scales provide a common form of intermediation to enable comparability of impact across incidents. Four of the impact categories assessed are in the context of the effects experienced by the reporting entity, with a fifth category (external) seeking to reflect impacts to the financial system or broader economy. External impacts may be more challenging for reporting entities to accurately assess based on their ability to form judgement on the downstream effects of an incident, though the normalised scales provide a means to approximate its magnitude. Additional descriptive details can also be provided through the **impact notes** information item at the end of the section.

All five impact categories are assessed by the reporting entity against a 5-point Likert scale (with an additional 'None' option to reflect absence of impact), with the option to record both the currently observed level of impact and the peak experienced over the course of the incident:

- **Financial**: financial losses due to fines, penalties, lost profits or diminished market share
- **Operational**: discontinued or reduced service levels, workflow disruptions, or supply chain disruptions
- **Reputational**: negative opinion or brand damage
- **Legal/Regulatory**: litigation liability and withdrawal of license of trade
- **External**: whereas the previous four scales describe internal facing impacts, impact external reflects the effects of the incident on the rest of the ecosystem

In addition, as supplemental information to express the magnitude of financial impact, **impact financial loss** provides the option to include an estimated quantification of total losses or costs associated with the incident in monetary terms.

Information Item	Purpose / Description	Field Type	Additional Syntax & Validation Rules, and Example Data
impact financial loss	(Minimum) total amount of gross direct and indirect costs and losses stemming from incident	Decimal	**Syntax** • Used to express minimum or precise financial loss, in denomination set by FIRE report currency. **Example** • *(At least or equal to) 250000*
impact financial loss max	Maximum total amount of gross direct and indirect costs and losses	Decimal	**Syntax** • Optional maximum financial loss to express range when estimating. **Example** • *(At most) 500000*

Information Item	Purpose / Description	Field Type	Additional Syntax & Validation Rules, and Example Data
impact financial	Describes current financial impacts experienced by the reporting entity	Enumerated	**Syntax** • Text (short) enumerated list, selected from values described in Annex J
impact financial peak	Describes peak financial impacts experienced by the reporting entity over the course of the incident	Enumerated	**Syntax** • Text (short) enumerated list, selected from values described in Annex J **Validation** • Cannot be lower value than impact financial
impact operational	Describes operational impacts experienced by the reporting entity	Enumerated	**Syntax** • Text (short) enumerated list, selected from values described in Annex K
impact operational peak	Describes peak operational impacts experienced by the reporting entity over the course of the incident	Enumerated	**Syntax** • Text (short) enumerated list, selected from values described in Annex K **Validation** • Cannot be lower value than impact operational
impact reputational	Describes reputational impacts experienced by the reporting entity	Enumerated	**Syntax** • Text (short) enumerated list, selected from values described in Annex L
impact reputational peak	Describes peak reputational impacts experienced by the reporting entity over the course of the incident	Enumerated	**Syntax** • Text (short) enumerated list, selected from values described in Annex L **Validation** • Cannot be lower value than impact reputational
impact legal / regulatory	Describes legal or regulatory impacts experienced by the reporting entity	Enumerated	**Syntax** • Text (short) enumerated list, selected from values described in Annex M
impact legal / regulatory peak	Describes peak legal or regulatory impacts experienced by the reporting entity over the	Enumerated	**Syntax** • Text (short) enumerated list, selected from values described in Annex M **Validation**

Information Item	Purpose / Description	Field Type	Additional Syntax & Validation Rules, and Example Data
	course of the incident		• Cannot be lower value than impact legal / regulatory
impact external	Describes perceived externalised effects of an incident on the rest of the ecosystem	Enumerated	**Syntax** • Text (short) enumerated list, selected from values described in Annex N
impact external peak	Describes peak external impacts over the course of the incident	Enumerated	**Syntax** • Text (short) enumerated list, selected from values described in Annex N **Validation** • Cannot be lower value than impact external

Geographic Spread

The sixth impact indicator included within the format is based on **geographic spread**, encompassing all affected parties by the incident. The degree of spread in the format has been normalised across five increasing geographic scales:

- **local**: affected parties are based within the same urban centre
- **regional**: affected parties are limited to a subset of territorial divisions within a jurisdiction e.g. counties
- **national**: affected parties have been identified throughout a single jurisdiction
- **multi-jurisdictional**: affected parties span more than one jurisdiction
- **global**: affected parties found in the majority of jurisdictions across multiple continents

For each selection, additional detail can be provided to describe a particular locale or region. When national or multi-jurisdictional options are selected, the descriptive information item conforms to ISO country code standard.

Information Item	Purpose / Description	Field Type	Additional Syntax & Validation Rules, and Example Data

impact geographic spread	Describes the extent to which the effects of the incident are being experienced, through increasing geographic scales	Array (key-value)	**Syntax**
			• Array of (one or more) pairs of Text (short), where the key entry is taken from this list:
			  ○ local
			  ○ regional
			  ○ national
			  ○ multi-jurisdictional
			  ○ global

Information Item	Purpose / Description	Field Type	Additional Syntax & Validation Rules, and Example Data
			Validation • If 'national' or 'multi-jurisdictional' selected, the value conforms to list of country codes using ISO 3166 alpha-2 encoding. • If 'local', 'regional', or 'global' selected, the value can be used to provide additional descriptive context as free text. • 'national' and 'global' entries can only be listed once. **Example** • *multi-jurisdictional, ES* • *multi-jurisdictional, DE* • *multi-jurisdictional, FR* • *multi-jurisdictional, IT*
impact notes	Provides more extensive description of impacts	Text (long)	**Example** • *The incident has received considerable media attention, and negative customer sentiment via social media channels.*

1.4. Incident Closure

The fourth and final set of information items related to institution-initiated reporting are confirmed once the incident has been closed and a post-incident review performed. Therefore, these information requirements are primarily 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:

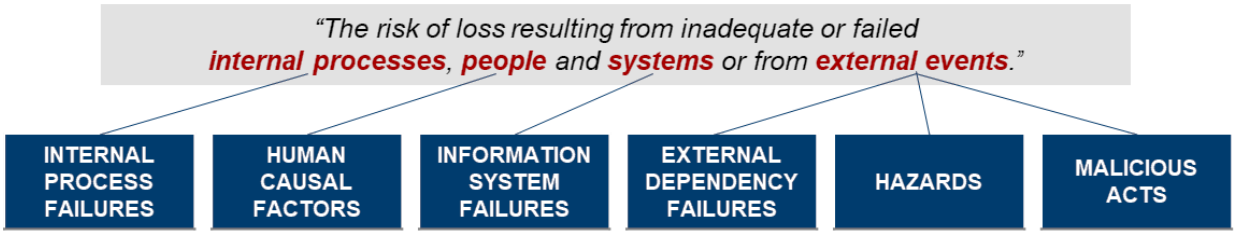
- **cause**, which explains why the incident took place and who or what may have caused it;
- **lessons identified and remedial activity**, which detail any vulnerabilities, and actions to be taken to address them; and
- **supplemental documentation**, to enable inclusion of file-based supporting materials.

1.4.1. 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 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 entities with early insight whilst the incident is still in progress.

To facilitate the enumeration of possible causes within the operational domain, a two-tier structure is adopted that seeks to align with the BCBS definition[26] of 'operational risk' as shown in **Figure 7**. At Level 2, a further 27 underlying causes are described in Annex O, offering a reasonable level of granularity both for the reporting entity to select from, and to support subsequent causal analysis. The Level 2 cause entries draw from a number of reputable sources (e.g. UNDRR, SEI, US Navy[27]) but have been significantly consolidated to simplify cause selection. Where the reporting entity is unable to identify an appropriate Level 2 cause to reflect the incident origin, the reporting entity can use a Level 1 cause family without further specificity (to avoid the use of 'other').

Figure 7. Level 1 cause type alignment to 'operational risk' definition



Against each possible cause, the reporting entity can indicate the causal strength associated with each cause identified:

- **root**: must have led to the incident
- **contributory**: could only lead to incident if combined with other failings

Alongside capturing the causation, the format also contains elements dedicated to recording the identity of the parties or forces (referred to as origin herein), whose actions led to the incident. The use of the term 'origin' is broader in scope than the concept of a threat actor[28] 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, e.g. force majeure.

- **origin:** a two-tier categorisation scheme to support subsequent analysis on the kinds of origins that lead to incidents at the reporting entity. At the category level, origin has been split into three groups, with type further elaborated in Annex P:
  - **internal**: organisational resource(s) or related entity (typically an individual) who is employed or contracted by the reporting entity and represents threat sources from within that entity
  - **third party**: entity with a pre-existing relationship with the reporting entity

---

26 BCBS (2004), *Basel II: International Convergence of Capital Measurement and Capital Standards: a Revised Framework*

27 Adaptations from sources including ; UN Office for Disaster Risk Reduction (UNDRR), *Sendai Framework for Disaster Risk Reduction;* Software Engineering Institute (SEI) (2014), *A Taxonomy of Operational Cyber Security Risks Version 2*; US Navy *HFACS (Human Factors Analysis and Classification System) Framework*;

28 FSB (2018), *Cyber Lexicon*, 12 November. (definition of *threat actor*)

- **external**[29]: entity has no pre-existing relationship with reporting entity

- **origin identity**: an optional attribute to name the origin, provided as free-text field. Where appropriate, a reporting entity may leverage recognised threat actor profile repositories to maintain consistent references to known entities.

- **vulnerabilities exploited**: where relevant, the reporting entity can specify which weaknesses, susceptibilities or flaws in assets or controls may have been exploited over the course of the incident.

An additional information item for **cause notes** is included to support more extensive description of either causes or the nature of the origins involved.

Information Item	Purpose / Description	Field Type	Additional Syntax & Validation Rules, and Example Data
cause(s) identified	Captures all causes that led or contributed to the incident	Container	**Validation** • At least one cause must have causal strength = 'root'
cause type	Categorisation of causes, spanning hazards, human causal factors, information system and process failures, external dependency failures, and malicious acts	Enumerated	**Syntax** • Text (short) enumerated list, selected from values in Annex O **Example** • *Malicious Acts - Ransomware*

causal strength	Describes the degree to which an identified cause contributed to the incident	Enumerated	**Syntax**
			• Text (short) enumerated list, selected from the following values:
			  ○ Root
			  ○ Contributory
			Example
			• *Root*

origin	High level categorisation of whose or what's actions caused or contributed to the incident	Enumerated	**Syntax** • Text (short) enumerated list, selected from values in Annex P. **Example** • *Outsourced service provider*
origin identity	Name or identifier of each suspected origin (where known), intended primarily	Array (key-value)	**Syntax** • Array of (one or more) Text (short) pairs in the form [name of identifier, value of identifier] **Validation**

29 Verizon (2019), *Vocabulary for Event Recording and Incident Sharing (VERIS)* (external actors variety)

Information Item	Purpose / Description	Field Type	Additional Syntax & Validation Rules, and Example Data
	to describe third party or external origins		• If "LEI" identifier is used, enforce validation rules in line with ISO 17442-1:2020 • If "" (blank / no identifier), free text allowed **Example** (fictitious) • *, HAL Corporation*
vulnerabilities exploited	Description of any weakness, susceptibility or flaw in assets or controls exploited during the course to the incident	Text (long)	**Example** (fictitious) • *Security flaw in a technology product*
cause notes	Provides more extensive description of causes and/or origins	Text (long)	**Example** (fictitious) • *Extended description of cause(s)*

1.4.2. 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 learned”. Identified lessons subsequently need to be implemented or applied, and then engrained within an institution before they can be considered as learned. Although the granularity of lessons identified is left for local implementers to determine, these should be comparable to the level of detail used to track remedial activity, with a focus on improvement and prevention of recurrence.

In the format, lessons identified consist of two parts:

- **lesson description**: describes the individual finding from the post-incident review
- **remedial action(s)**: captures every action being undertaken by the reporting entity to address each finding, alongside an estimated remediation completion date associated with each action, using the ISO 8601:2019 format to represent dates (YYYY-MM-DD)

The combination of these information items provides both the reporting and receiving entity with the necessary remediation planning information to monitor progress and to subsequently evaluate whether causes have been adequately addressed.

Information Item	Purpose / Description	Field Type	Additional Syntax & Validation Rules, and Example Data
lesson(s) identified	Captures each lesson identified (not ‘learned’) from the reporting	Container	

Information Item	Purpose / Description	Field Type	Additional Syntax & Validation Rules, and Example Data
	entity's post-incident review		
lesson description	Describes an individual finding from the post-incident review	Text (long)	**Example** • *Lesson 1 identified from incident*
remedial action(s)	Describes one or more actions being undertaken by the reporting entity to address the finding, and an estimated remediation completion date for each action	Array (key-value)	**Syntax** • Array of (one or more) pairs in the form [Date, Text (Long)] • Date uses ISO 8601 format: YYYY-MM-DD **Validation** • Date stamp can be omitted, in the future or the past (e.g. may have been completed by time final report issued) **Example** • *2024-09-13, Description of Action 1 linked to Lesson 1* • *2025-03-22, Description of Action 2 linked to Lesson 1*

1.4.3. Supplemental Documentation

As not all information can be captured through structured text-based information items, the format includes a mechanism for incorporating 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 entities may wish to have additional content submitted at other points in the incident lifecycle.

To enable this process, the format supports various methods for the exchange of supplemental information, either within the FIRE message itself or as a complementary process, using the following information items:

- **attachment method**: the method selected by the reporting entity to exchange supplemental information, chosen from:
  - **embedded**: attachment(s) contained within the message using the attachment embedded information item;
  - **email**: attachment(s) communicated to receiving entities by email separately from the FIRE message, with attachment reference(s) used to convey email title, sender and/or recipient details;
  - **file transfer**: attachment(s) communicated to receiving entities by file transfer (e.g. FTP/SFTP) separately from the FIRE message, with attachment reference(s) used to specify file name(s) and where transmitted file(s) can be located; and

- **externally hosted**: attachment(s) made available to receiving entities for separate download from a specified location, with attachment reference(s) used to specify hosting location (e.g. URL), where to find relevant access credentials, and file name(s) references.

- **attachment instructions**: an unstructured long text field to describe each attachment and how non-embedded files can be retrieved / accessed using the selected method.

- **attachment embedded**: an array of Base64 binary-encoded files used to support the upload and inclusion of attachments within the FIRE message being exchanged with receiving entities.

Information Item	Purpose / Description	Field Type	Additional Syntax & Validation Rules, and Example Data

attachment method	Describes the method employed to provide supplemental information regarding the incident	Enumerated	**Syntax**
			• Text (short) enumerated list, selected from the following values:
			  ○ embedded
			  ○ email
			  ○ file transfer
			  ○ externally hosted
			Example
			• *Embedded*

attachment instructions	Describes the file name(s) and additional retrieval instructions for non-embedded exchange of attachments	Text (long)	**Example** • *Attachments will be communicated to all report recipients with the following email details:* ***From**: contact@reporting-entity.com* ***Title**: FIRE Incident Report ID123456789* ***Attachment(s)**: File1.pdf, File2.pdf, File3.pdf*
attachment embedded	Provides option for additional details via upload of bespoke documentation	Array (list)	**Syntax** • Array of one or more files of type Attachment, stored using Base64 encoding **Validation** • There may be some maximum file size considerations, but this constraint would be linked to individual local implementations **Example** • *Encoded representation of commonly used file formats (e.g. DOC, PDF, PPT, etc…)*

Annex A: Standardised Field Types

Field Name	Type	Description	Limits / Format	Example
Array (key-value)	List	List of key/value pairs		[("Integer","Text(Short)")]
Array (list)	List	List with a number of elements in a specific order—typically of the same type		["Enum1","Enum2","Enum3"]
Attachment	Binary	Binary encoded file converted to Base64 (or equivalent)		
Boolean	Boolean	True or false values	0 (false), 1 (true)	1
Container	Container	Collection of one or more fields with related purpose		
Date	Date/Time	Date using the ISO 8601 format	YYYY-MM-DD	2023-12-12
Datetime	Date/Time	Date and time together using the ISO 8601 format	YYYY-MM-DDTHH:mm:ssTZD	2024-01-25T14:17+00:00
Decimal	Numeric	Numeric data type for numbers with fractions, conformant ISO/IEC 60559:2020	binary32 format	7.04
Duration	Date/Time	Time interval using the ISO 8601 format	P[n]Y[n]M[n]DT[n]H[n]M	PT3H15M
Enumerated	List	Small set of predefined unique values (elements or enumerators) that can be string-based or numeric	Single selection from the list	Value 1
Integer	Numeric	Numeric data type for numbers without fractions	Long signed (32-bit) format	13
Percentage	Numeric	Decimal with limited values (between 0 and 1 inclusive)	>=0 and <=1	0.46
Text (Email)	String	String conformant with RFC5322 format	localpart "@" domain	john.smith@email.com
Text (Long)	String	A long text field for paragraphs of text, with UTF-8 encoding	65,535 characters	Multiple paragraphs…
Text (Short)	String	A short text field for titles and names, with UTF-8 encoding	255 characters, no newline	A short sentence / statement
Text (Telephone)	String	String conformant with E.164 standard: +[country code][subscriber number] with maximum 15 numbers	Regex: /^\+[1-9]\d14$/	+14151234567

Annex B: Reporting Phase Optionality for Institution-Initiated Reporting

Information Item Name	**Initial** *(open)*	**Initial** *(resolved)* **Intermediate** *(open)* **Intermediate** *(resolved)*	**Initial** *(closed)* **Final** *(resolved)* **Final** *(closed)*
MESSAGE HEADER			
FIRE version	Essential	Essential	Essential
FIRE report type	Essential	Essential	Essential
FIRE report language	Essential	Essential	Essential
FIRE report currency	Essential	Essential	Essential
REPORTING DETAILS			
REPORTING ENTITY			
entity name	Essential	Essential	Essential
global identifier(s)	Optional	Optional	Optional
local identifier(s)	Optional	Optional	Optional
ultimate parent name	Optional	Optional	Optional
entity type(s)	Essential	Essential	Essential
entity country	Optional	Optional	Optional
RECEIVING ENTITY			
recipient identifier(s)	Essential	Essential	Essential
recipient history	Optional	Optional	Optional
forwarding sender	Not collected	Not collected	Not collected
forwarding recipient(s)	Not collected	Not collected	Not collected
CONTACT DETAILS			
entity contact(s)	Essential (1 or more)	Essential (1 or more)	Essential (1 or more)
contact type	Essential	Essential	Essential
contact name	Essential	Essential	Essential
contact email	Essential	Essential	Essential
contact phone	Essential	Essential	Essential
contact role	Optional	Optional	Optional
contact department	Optional	Optional	Optional
contact recipient	Optional	Optional	Optional
INCIDENT DETAILS			
REFERENCES			
entity internal incident ID	Optional	Optional	Optional
entity related incident ID(s)	Optional	Optional	Optional
INCIDENT			
report phase	Essential	Essential	Essential
incident status	Essential	Essential	Essential
incident title	Essential	Essential	Essential
incident description	Essential	Essential	Essential
incident type	Optional	Essential	Essential

Information Item Name	Initial *(open)*	Initial *(resolved)* Intermediate *(open)* Intermediate *(resolved)*	Initial *(closed)* Final *(resolved)* Final *(closed)*
incident artefact(s)	Optional	Optional	Optional
incident discovery method	Optional	Essential	Essential
incident reporting trigger(s)	Optional	Essential	Essential
incident estimated resolution timeframe	Optional	Optional	Not applicable
incident estimated resolution timeframe max	Optional	Optional	Not applicable
CHANGE(S) SINCE PREVIOUS REPORT			
actions taken	Optional	Essential	Essential
actions planned	Optional	Essential	Not applicable
public reaction	Optional	Optional	Essential
comms issued	Optional	Optional	Essential
bodies notified	Optional	Optional	Essential
DATE / TIME MARKERS			
time of report	Essential	Essential	Essential
time of occurrence	Optional	Optional	Optional
time of detection	Optional	Optional	Essential
time of resolution	Not applicable	Essential	Essential
time of closure	Not applicable	Not applicable	Essential
time of next update	Optional	Optional	Not applicable
IMPACT ASSESSMENT			
SEVERITY RATING			
entity severity	Optional	Optional	Optional
standardised severity	Essential	Essential	Essential
AFFECTED PARTIES			
affected parties	Optional	Optional	Essential
related affected entities	Optional	Optional	Essential
affected notes	Optional	Optional	Optional
SERVICES AND RESOURCES			
service(s) affected	Optional	Essential	Essential
service name	Optional	Essential	Essential
service type	Optional	Essential	Essential
service critical	Optional	Optional	Optional
service disruption type	Optional	Essential	Essential
service downtime	Optional	Essential	Essential
service downtime max	Optional	Optional	Optional
affected end user number	Optional	Essential	Essential
affected end user number max	Optional	Optional	Optional

Information Item Name	**Initial** *(open)*	**Initial** *(resolved)* **Intermediate** *(open)* **Intermediate** *(resolved)*	**Initial** *(closed)* **Final** *(resolved)* **Final** *(closed)*
affected end user percentage	Optional	Essential	Essential
affected end user percentage max	Optional	Optional	Optional
affected transaction type	Optional	Optional	Optional
Affected transaction number	Optional	Optional	Optional
affected transaction number max	Optional	Optional	Optional
affected transaction percentage	Optional	Optional	Optional
affected transaction percentage max	Optional	Optional	Optional
affected transaction value	Optional	Optional	Optional
affected transaction value max	Optional	Optional	Optional
Resource(s) affected	Optional	Optional	Essential
resource type	Optional	Optional	Essential
resource affected properties	Optional	Optional	Essential
service / resource notes	Optional	Optional	Optional
IMPACT			
impact financial loss	Optional	Optional	Optional
impact financial loss max	Optional	Optional	Optional
impact financial	Optional	Optional	Optional
impact financial peak	Optional	Optional	Optional
impact operational	Optional	Optional	Optional
impact operational peak	Optional	Optional	Optional
impact reputational	Optional	Optional	Optional
impact reputational peak	Optional	Optional	Optional
impact legal / regulatory	Optional	Optional	Optional
impact legal / regulatory peak	Optional	Optional	Optional
impact external	Optional	Essential	Essential
impact external peak	Optional	Optional	Optional
impact geographic spread	Optional	Essential	Essential
impact notes	Optional	Optional	Optional
INCIDENT CLOSURE			
CAUSE			
cause(s) identified	Optional	Optional	Essential
cause type	Optional	Optional	Essential

Information Item Name	**Initial** *(open)*	**Initial** *(resolved)* **Intermediate** *(open)* **Intermediate** *(resolved)*	**Initial** *(closed)* **Final** *(resolved)* **Final** *(closed)*
causal strength	Optional	Optional	Optional
origin	Optional	Optional	Essential
origin identity	Optional	Optional	Optional
vulnerabilities exploited	Optional	Optional	Optional
cause notes	Optional	Optional	Optional
LESSONS			
lesson(s) identified	Not applicable	Not applicable	Essential
lesson description	Not applicable	Not applicable	Essential
remedial action(s)	Not applicable	Not applicable	Essential
SUPPLEMENTAL DOCUMENTATION			
attachment method	Optional	Optional	Optional
attachment instructions	Optional	Optional	Optional
attachment embedded	Optional	Optional	Optional

Annex C: Incident Type

Incident Type	Definition	Example(s)
Business Disruption, System or Execution Failure	Any type of operational incident that disrupts the provision of an entity's activities, functions or services	Technology failure, loss of third-party service, Denial of Service (DoS), malware, natural disaster
Compromise* *(non-disruptive)*	(Non-disruptive) Violation of the security of an information system	Account compromise, intrusion, defacement, resource hijacking
Data Breach*	Compromise of security that leads to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to data transmitted, stored or otherwise processed	Data leakage, data loss, data manipulation
Financial Theft / Fraud	A deliberate act to obtain unauthorised financial benefit	Theft of funds via digital channel
Information Disorder	The spread of false or reality-based information, whether malicious or not	Misinformation, disinformation, malinformation

**FSB Cyber Lexicon definitions*

Annex D: Incident Discovery Method

Discovery Method		Description
External	Actor Disclosure	Announced / informed by threat actor
	Authority / Agency	Reported by (national) competent authority e.g. financial authority, cyber security agency
	Law Enforcement	Reported by domestic or international law enforcement agency (LEA) e.g. police, national crime agency, Interpol
	Third Party	Reported by one of the reporting entity's external dependencies e.g. managed service provider, vendor
	Customer / Client	Reported by consumer(s) of the reporting entity's services e.g. counterparty
	Peer / Competitor	Reported by another regulated entity e.g. via collaborative information sharing platform
	External Audit	Discovered following a review performed by external auditors e.g. perimeter scanning service provider
	Monitoring service	Reported by external monitoring provider e.g. security event monitoring service
	Unrelated party	Reported by party with no relationship to the reporting entity e.g. bug bounty hunter
	Unknown	Reported by anonymous or unidentified external entity
Internal	Incident Response	Discovered while responding to another incident
	Security Operations Centre	Discovered by dedicated security function as part of business-as-usual activities
	Existing Detection Technique	Discovered using existing monitoring tools e.g. intrusion detection, log monitoring
	Internal Audit	Discovered following a review performed by internal auditors
	Staff	Reported by contracted staff at reporting entity
	Unknown	Reported by anonymous or unidentified internal entity
Unknown		Reported from unknown source
Other		*(include within incident description)*

Annex E: Standardised Severity

Severity Level *(incl. description and step change transition statements)*		**Additional context** *(may be observed)*
Nil	Not requiring any form of incident response	
▼ *Incident response managed as part of business-as-usual activities*		
Negligible	Localised incident being handled in line with **standard operating procedures** without need for bespoke intervention	• Incident handled using established procedures without the need for tailored response or supplemental resources
▼ *Specific and coordinated response required to manage incident*		
Low	**Escalated** incident response mode within relevant functional units	• Escalation within affected functional unit (e.g. operations / technology / SOC) is sufficient for response • May designate a named incident coordinator or incident response team (IRT) • Crisis escalation procedures have not been activated
▼ *Invocation of crisis management arrangements*		
Medium	**Crisis management** arrangements are invoked	• Need for coordinated organisational response • Constant internal communication flows • Activation of crisis communication strategies
▼ *Crisis escalation to most senior level*		
High	Escalated to the **most senior crisis command structure** that holds ultimate responsibility for the handling and outcome of the incident	• Strategic crisis response led from most senior command structure within affected entity • Significant threat(s) to the safety and soundness of the affected entity
▼ *Crisis management becomes a collective responsibility*		
Extreme	Incident is treated with the utmost severity, where the affected entity's **survival or orderly functioning** of the sector is at stake	• Sectoral crisis response arrangements have been invoked • Real and imminent risk to the safety and soundness of the affected entity

Annex F: Service Disruption Type

Service disruption type		Description
Availability Loss	Total	Service is completely unavailable to its external end users
	Partial	A subset of the service's features/components is unavailable to its external end users
	Intermittent	Service is occasionally unavailable (total or partial) at either regular or irregular intervals
	Degradation	Service is operating below predefined acceptable service levels
Integrity Loss	Manipulation	Creation, addition, duplication, modification, re-sequencing or deletion of information related to service
	Corruption	Information related to service in unreadable, but recoverable or can be reconstituted
	Destruction	Information related to service has been irrevocably lost
Confidentiality Loss	Unintended / Unauthorised disclosure	The exposure of information to entities not authorised access to the information (e.g. data leakage)
	Unauthorised acquisition	Gaining access to and/or retrieving information without valid authorisation (e.g. data exfiltration, interception)
Loss of Trust	Impersonation	Service identity is assumed or mimicked by an unauthorised entity (e.g. cloned identity, man-in-the-middle)
	Disinformation	Intentional dissemination of false information, with an end goal of misleading, confusing or manipulating an audience
	Rumour / Speculation	Spread of information without confirmation of its veracity
Unknown		Nature of the service disruption yet to be confirmed
Other		Service disruption type does not match pre-defined categories

Annex G: ISO 20022 Business Areas[30]

Business Area (BA) Grouping	Business Areas within ISO 20022
Card Payments & Related Transactions	Acceptor to Acquirer Card Transactions, Acquirer to Issuer Card Transactions, Sale to POI Card Transactions, ATM Card Transactions, Card Administration, POI Management, ATM Management, Fee collection, Payment Token Management, Network Management, File Management, Settlement Reporting, Fraud Reporting and Disposition
Payments & Cash Management	Payments Initiation, Payments Clearing and Settlement, Cash Management, Payments Remittance Advice
Trade Services	Trade Services Initiation, Trade Services, Trade Services Management
Securities	Securities Issuance, Securities Trade Initiation, Securities Trade, Securities Clearing, Securities Settlement, Securities Management, Securities Events
Foreign Exchange	Foreign Exchange Trade Initiation, Foreign Exchange Trade, Foreign Exchange Management
Bank Loan/Deposit	Bank Loan Trade Initiation, Bank Loan Trade, Bank Loan Management
Derivatives	Derivatives Trade Initiation, Derivatives Trade, Derivatives Management
Commodities	Commodities Trade Initiation, Commodities Trade, Commodities Management
Syndicated Loans	Syndicated Loan Initiation, Syndicated Loan, Syndicated Loan Management
Miscellaneous/Generic	Account Management, Administration, Authorities, Collateral, Reference Data
Not Applicable	No transaction type associated with affected service
Other	Other type of transaction not covered by ISO 20022

[30] ISO (2017), *ISO 20022 Business Areas* (augmented with not applicable and other types)

Annex H: Resource Type

Resource type		Description / Examples (non-exhaustive)
People		Employees (and their associated skill, talents or abilities)
Property		Buildings, equipment, machinery, vehicles, land, office space, office equipment, furnishings
Technology	ICT (Information & Communication Technology) hardware	Storage equipment, servers, mainframes, back-up facilities, desktop equipment, network equipment, communications, voice services
	OT (Operational Technology) hardware	Building management control systems, SCADA systems, Industrial Controls Systems (ICS), Distributed Controls Systems, Intrusion Detection Systems, Physical Access Control Systems, Emergency Management Systems
	Software	Operating systems (incl. virtual), applications (internal or third-party developed), middleware components, web components
Information	Datastore	Persistent and structured repositories of information (e.g. RDBMS, key/value stores, document stores)
	File-based data	Electronic or physical store of information
	Code	In-house developed
	Third party library	Purchased or open-source library used by reporting entity
	Archived information	Collection of data held within a repository for long-term retention

Annex I: Resource Properties[31]

Property	Description
Availability	property of being accessible and usable on demand by an authorised entity
Integrity	property of accuracy and completeness
Confidentiality	property that information is neither made available nor disclosed to unauthorised individuals, entities, processes or systems
Authenticity	property that an entity is what it claims to be
Accountability	property that ensures that the actions of an entity may be traced uniquely to that entity
Non-repudiation	ability to prove the occurrence of a claimed event or action and its originating entities
Reliability	property of consistent intended behaviour and results

31 FSB (2018). from definition of *cyber security*

Annex J: Financial Impact Scale

Impact Level *(incl. description and step change transition statements)*		**Additional context** *(may be observed)*
None	No financial impact observed	
▼ *Financial impact observed or expected*		
Insignificant	**Inconsequential** financial loss recorded	• May involve minimal expense that is absorbed within existing budgets
▼ *Losses extend beyond typical operating parameters for affected business line(s)*		
Minor	**Limited** financial losses arising from direct or indirect costs associated with the incident	• Financial impact can be absorbed using entity-wide provisions for operational risk loss events • Not yet detrimental to overall entity profitability
▼ *Losses become an organisational concern and draw on available sources of funding*		
Moderate	Considerable financial losses occurring, **but can be absorbed**	• Negatively impacting on entity profitability • Losses can be contained through cost-cutting measures • Liquidity adequacy and/or capital position is deteriorating
▼ *Entity is no longer able to absorb mounting losses*		
Substantial	Entity in **financial difficulty**, with increased exposure to liquidity risk or losses that can no longer be absorbed	• Increasing risk that the entity will make use of external (e.g., central bank) funding or perform material adjustments to business model to satisfy liquidity requirements • Capital requirements may be breached if recovery plan is unsuccessful
▼ *Entity is no longer able to adequately function without external intervention*		
Severe	Entity in **financial distress or insolvent**, and unable to meet or pay its financial obligations	• Entity on verge of no longer being viable (gone concern) • Imminent possibility of one or more authorities withdrawing authorisation and/or resolution, winding-up or insolvent run-off being triggered

Annex K: Operational Impact Scale

Impact Level *(incl. description and step change transition statements)*		**Additional context** *(may be observed)*
None	No operational impact observed	
▼ *Operational impact observed or expected*		
Insignificant	Degradation in provision or safeguarding of non-critical services or resources	• Disruption to underlying resources managed using entity's existing recovery arrangements • Compromise of information that has no lasting effect
▼ *Non-critical failure*		
Minor	**Failure or consequential compromise** of non-critical services or resources OR **limited degradation** in provision of critical services or resources	• Non-critical services or resources affected • Limited deterioration in provision of critical services and / or availability of resources • Compromise of information has limited implications
▼ *Disruption to critical services or resources*		
Moderate	Provision or safeguarding of one or more **critical** services or resources is adversely affected	• Deterioration in provision of critical services and/or availability of resources • No large-scale impact in terms of proportion of resources affected • Compromise of information has noticeable implications in terms of sensitivity or volume
▼ *Substantive intolerable dysfunction*		
Substantial	Critical services or resources affected such that **key business objectives are not met**	• Tolerable levels of disruption for critical service(s) breached • Recovery is possible but has a degree of uncertainty, complexity and effort • Large scale impact in terms of proportion of resources affected • Compromise of information is extensive in terms of sensitivity or volume
▼ *No longer able to operate core business function(s)*		
Severe	Sustained operational impact preventing the entity **from achieving its mission**	• Irrevocable loss of critical services or resources which prevents the entity from operating (e.g. operational paralysis) • All recovery options are exhausted

Annex L: Reputational Impact Scale

Impact Level *(incl. description and step change transition statements)*		**Additional context** *(may be observed)*
None	No reputational impact observed	
▼ *Adverse reaction associated with incident is identified*		
Insignificant	**Isolated** instance(s) of criticism / negative reaction from a small number of external parties	• Limited or localised negative coverage or customer frustration / complaint • No press exposure • No notable effect on reputation / image • Can be handled by the entity's standard communication protocols or complaint handling processes
▼ *Gathering negative momentum broadening into local mainstream coverage*		
Minor	Multiple **regional** instances of criticism / negative reaction by external parties	• Temporary coverage by local media • Local public opinion aware • Social media trending • Minor short-term, but recoverable, effect on reputation • Specific communications issued by affected entity in response to incident • Few complaints received from customers
▼ *Escalating concern which triggers national interest or official critique*		
Moderate	Mounting public, institutional or market concern reflecting a deterioration in **stakeholder confidence**	• Extended local or one-time national media coverage within the entity's primary region of operation • Social media trending with moderate levels of engagement and visibility • Negative commentary and interest from officials (e.g. political or authority) representatives • No loss of core customer trust but repetitive complaints received from customers
▼ *Loss in brand value, prospects, or market share*		
Substantial	Potential for reputational damage driven by **widespread** social, national, and mainstream media coverage or public scrutiny	• Persistent and intense negative media coverage, expanding to front page articles or international media interest • Loss of confidence amongst customers, peer group or investors • Public censure from official representatives • Large numbers of repetitive complaints received from different customer segments

Impact Level *(incl. description and step change transition statements)*		**Additional context** *(may be observed)*
▼ *Extensive loss of trust or confidence in entity's ability to meet external end user or market expectations*		
Severe	**Reputational damage** as a result of prolonged social, national and mainstream media coverage or public scrutiny	• Long-term or severe repercussions for brand or market value, potentially beyond repair • Large-scale loss of customer trust, potential shareholder and regulatory actions • Reputational impacts extending to affiliated entities, markets or locale

Annex M: Legal / Regulatory Impact Scale

Impact Level *(incl. description and step change transition statements)*		**Additional context** *(may be observed)*
None	No legal or regulatory impact observed	
▼ *Legal or regulatory impact observed or expected*		
Insignificant	Breach of legislation, contract or policy that **does not have any penalty or litigation impact**	• Procedural breaches with no direct violation of laws or regulations • No regulatory impact or consequences for the breach
▼ *Breach that may affect the entity or its contractual obligations*		
Minor	Breach of legislation, contract or policy that may have an impact on its contractual or compliance obligation **but with no long-lasting effect**	• Breach limited to non-critical procedures / arrangements with stakeholders • Isolated or technical violations of regulations • May result in formal contact from relevant authorities to appraise and monitor the situation
▼ *Noticeable non-compliance or breach of obligations affecting some operations or stakeholders*		
Moderate	Legal obligation breach or regulatory non-compliance causing noticeable impact and **requiring measures to prevent recurrence**	• Significant single violation or pattern of issues • Relevant authorities may engage with affected parties to assess entity-specific or sectoral impacts for corrective action(s)
▼ *Significant deviation(s) from compliance, significantly affecting operations or stakeholders*		
Substantial	Major or repeated breach of legal / regulatory obligation(s) with potential for **serious compliance exposure or legal liability**	• Relevant authorities may intervene to minimise risks to their objectives
▼ *Violation has potential to threaten the entity's viability*		
Severe	Extended legal or regulatory violation(s) with potential for **damaging or lasting consequences** for affected entity and/or its senior management	• Extreme non-compliance and/or severely affecting stakeholders • May require long-term strategic review or overhaul of internal controls and policies

Annex N: External Impact Scale

Impact Level *(incl. description and step change transition statements)*		**Additional context** *(may be observed)*
None	No externalised impact observed	
▼ *External parties temporarily inconvenienced by incident*		
Insignificant	Momentary expressions of **dissatisfaction** with the obligation of affected entity	• Short-term consumer inconvenience • Alternate channels or mechanisms available to achieve external end user outcomes
▼ *External parties directly or indirectly affected such that desired activities are impaired*		
Minor	Incident leads to a **disproportionate level** of disruption or difficulty for external parties	• Continued provision of critical services within tolerable levels despite observable disruption
▼ *Failure to meet stakeholder needs or safeguard their interests*		
Moderate	Affected entity **no longer meeting expectations** of one or more stakeholder groups	• Failure to meet service level obligations • Mounting consumer detriment (disadvantaged and/or dissatisfied) • Results in restricted access to financial services
▼ *Impacts leading to second-order (or greater) contagious effects for other entities*		
Substantial	Incident leads to resultant failures at, impairment of, or **damaging outcomes** for, dependent stakeholders	• Potential for wider ecosystem consequences • Actual harm to consumers, clients, or market integrity or competitiveness • Poses a risk to policyholder protection • Risks stability, integrity and/or confidence in the financial system
▼ *Incident is beyond the control of affected entities*		
Severe	**Impending risk** to orderly running of affected entities, their counterparties, or financial system as a whole	• Serious harm to consumer or client interests • Serious financial consequences for the financial system, other market participants or broader economy

Annex O: Cause Type

Cause Type (Level 1 and 2)		**Description**
Internal Process Failures	Process design and maintenance	Failure to adequately design, document, or implement end-to-end processes (including inputs, outputs, flow, measurements) and subsequently review and maintain on a periodic basis, in line with stakeholder expectations
	Roles, responsibilities, and process ownership	Insufficient definition and understanding of process stakeholder roles and responsibilities as well as poor definition of process ownership or poor governance practices
	Process monitoring and issue escalation	Failure to adequately notify, review, respond to, or escalate abnormal or unexpected conditions about the operation of processes for action by the appropriate personnel.
	Service level agreements	The lack of agreement among process stakeholders on service expectations that causes a failure to complete expected actions
		Unspecified internal process failure
Human Causal Factors	Human error	Failure in execution through: • incorrect action (mistake), • lack of proper knowledge (uninformed), • improper choices (misjudgement), • hasty performance (omission), • failure to act (inaction), • adverse personal conditions (fitness for duty), or • intentional deviation from expected behaviours (contravention)
	Adverse work environment	Deficiencies in operating environment or organisational culture which adversely affect human performance
	Management failure	Failure to provide adequate oversight, correct known problems, or supply appropriate human, monetary, or equipment resources necessary to support operations
		Unspecified human causal factor
Information System Failures	Design, development, and testing	Failures resulting from improper or inadequate definition of requirements, failure to adhere to requirements during development, implementation / configuration errors, and ineffective or atypical testing
	Change control	Changes made to information systems or their configuration by a process lacking appropriate authorisation, review, and rigour
	Capacity and performance	Inability to handle a given load or volume of information or inability to complete instructions or process information within acceptable parameters (speed, power consumption, heat load, etc.)
	Maintenance and obsolescence	Failure resulting from inadequate or insufficient maintenance of information system components, or its operation beyond supported service life
	Systems complexity or integration	System intricacy or a large number or interrelationships between components or failure of various components of the system to function together or interface correctly

Cause Type (Level 1 and 2)		**Description**
		Unspecified information system failure
External Dependency Failures	Operational failure (excl. security)	Failure to meet expectations or contractual obligations for provision of services or goods, due to ineffective or failed internal processes, people, controls or systems
	Security failure	Compromise or data breach at third party or within supply chain which adversely affect assets that have value to the institution
	Business-driven failure	External dependency failure resulting from provider's financial inadequacy, legal or regulatory non-compliance, detrimental action(s) leading to reputational damage, or taking incompatible strategic decisions on service provision
		Unspecified external dependency failure
Hazards	Natural hazard	Natural process or phenomenon that may cause loss of life, injury or other health impacts, property damage, loss of livelihoods and services, social and economic disruption, or environmental damage (including meteorological, hydrological, geological, and naturally occurring biological and chemical hazards, as well as space weather)
	Human-induced hazard	Hazard brought about entirely or predominantly by human activities and choices, and have the potential to endanger exposed populations and environment (including environmental, technological, and societal hazards)
		Unspecified hazard
Malicious Acts	DoS / DDoS	**Denial of Service (DoS)**: Prevention of authorised access to information or information systems; or the delaying of information system operations and functions, with resultant loss of availability to authorised users. **Distributed Denial of Service (DDoS)**: A denial of service that is carried out using numerous sources simultaneously.
	Identity theft	Wrongfully obtaining and using another person's personal data in some way that involves fraud or deception, typically for economic gain
	Insider threat	A deliberate act from an insider threat to damage, disrupt or gain unauthorised access to assets
	Malware	Software designed with malicious intent containing features or capabilities that can potentially cause harm directly or indirectly to entities or their information systems.
	Physical manipulation, damage, theft and loss	Actions which adversely affect an entity's assets in the physical (i.e. tangible, real-world) environment
	Ransomware	Malware that is used to commit extortion by impairing the use of an information system or its information until a ransom demand is satisfied.
	Resource hijacking	Leveraging the resources of co-opted information systems to complete resource-intensive tasks, which may impact system and/or hosted service availability.
	Social engineering (including phishing)	**Social engineering**: A general term for trying to deceive people into revealing information or performing certain actions. **Phishing**: A digital form of social engineering that attempts to acquire private or confidential information by pretending to be a trustworthy entity in an electronic communication.

Cause Type (Level 1 and 2)		**Description**
	Spam	Abuse of electronic messaging systems to indiscriminately send unsolicited bulk messages
	Web application targeting	Actions which compromise the cyber security of a web-based application or service (e.g. watering hole attack, exploitation of websites, Internet-accessible applications or remote access services violations)
		Unspecified malicious act

Annex P: Origin

Origin (with sub-type where appropriate)	
Internal	
Third Party	Intragroup entity
	Outsourced service provider
	Non-outsourced third party
	Supply chain - Fourth (or greater) party
	Critical infrastructure / Utility provider
External	Force majeure (nature and chance)
	Threat actor (malicious intent)
	Financial market participant
	Customer / consumer
Unknown	
Other	