FSB FINANCIAL STABILITY BOARD

Recommendations to Achieve Greater Convergence in Cyber Incident Reporting

Final Report

13 April 2023

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

Contact the Financial Stability Board

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

Table of Contents

Executive summary

Cyber incidents are rapidly growing in frequency and sophistication. At the same time, the cyber threat landscape is expanding amid digital transformation, increased dependencies on third-party service providers and geopolitical tensions. The interconnectedness of the global financial system makes it possible that a cyber incident at one financial institution (FI) (or an incident at one of its third-party service providers) could have spill-over effects across borders and sectors.

Recognising that timely and accurate information on cyber incidents is crucial for effective incident response and recovery and promoting financial stability, the G20 asked the FSB to deliver a report on achieving greater convergence in cyber incident reporting (CIR). To meet this call, the FSB conducted work to promote greater convergence in CIR in three ways: (i) setting out recommendations to address the issues identified as impediments to achieving greater harmonisation in incident reporting; (ii) enhancing the Cyber Lexicon[1] to include additional terms related to CIR as a 'common language' is necessary for increased convergence; and (iii) identifying common types of information that are submitted by FIs to authorities for CIR purposes, which culminated in a concept for a common format for incident reporting exchange (FIRE) to collect incident information from FIs and use between themselves. FIRE would be flexible to allow a range of adoption choices and include the most relevant data elements for financial authorities.

Drawing from the FSB's body of work on cyber, including engagement with external stakeholders, this report sets out recommendations that aim to promote convergence among CIR frameworks, while recognising that a one-size-fits-all approach is not feasible or preferable. Financial authorities and FIs can choose to adopt these recommendations as appropriate and relevant, consistent with their legal and regulatory framework.

Recommendations:

1. **Establish and maintain objectives for CIR**. Financial authorities should have clearly defined objectives for incident reporting, and periodically assess and demonstrate how these objectives can be achieved in an efficient manner, both for FIs and authorities.

2. **Explore greater convergence of CIR frameworks**. Financial authorities should continue to explore ways to align their CIR regimes with other relevant authorities, on a cross-border and cross-sectoral basis, to minimise potential fragmentation and improve interoperability.

3. **Adopt common data requirements and reporting formats**. Financial authorities should individually or collectively identify common data requirements, and, where appropriate, develop or adopt standardised formats for the exchange of incident reporting information.

4. **Implement phased and incremental reporting requirements**. Financial authorities should implement incremental reporting requirements in a phased manner, balancing the authority's need for timely reporting with the affected institution's primary objective of bringing the incident under control.

---

1 FSB (2023), *Cyber Lexicon: Updated in 2023*, April.

5. **Select appropriate incident reporting triggers**. Financial authorities should explore the benefits and implications of a range of reporting trigger options as part of the design of their CIR regime.

6. **Calibrate initial reporting windows**. Financial authorities should consider potential outcomes associated with window design or calibration used for initial reporting.

7. **Provide sufficient details to minimise interpretation risk.** Financial authorities should promote consistent understanding and minimise interpretation risk by providing an appropriate level of detail in setting reporting thresholds, using common terminologies and supplementing CIR guidance with examples.

8. **Promote timely reporting under materiality-based triggers**. Financial authorities that use materiality thresholds should consider finetuning threshold language, or explore other suitable approaches, to encourage prompt reporting by FIs for material incidents.

9. **Review the effectiveness of CIR and cyber incident response and recovery (CIRR) processes.** Financial authorities should explore ways to review the effectiveness of FIs' CIR and CIRR processes and procedures as part of their existing supervisory or regulatory engagement.

10. **Conduct ad-hoc data collection**. Financial authorities should explore ways to complement CIR frameworks with supervisory measures as needed and engage FIs on cyber incidents, both during and outside of live incidents.

11. **Address impediments to cross-border information sharing**. Financial authorities should explore methods for collaboratively addressing legal or confidentiality challenges relating to the exchange of CIR information on a cross-border basis.

12. **Foster mutual understanding of benefits of reporting**. Financial authorities should engage regularly with FIs to raise awareness of the value and importance of incident reporting, understand possible challenges faced by FIs and identify approaches to overcome them when warranted.

13. **Provide guidance on effective CIR communication**. Financial authorities should explore ways to develop, or foster development of, toolkits and guidelines to promote effective communication practices in cyber incident reports.

14. **Maintain response capabilities which support CIR**. FIs should continuously identify and address any gaps in their cyber incident response capabilities which directly support CIR, including incident detection, assessment and training on a continuous basis.

15. **Pool knowledge to identify related cyber events and cyber incidents.** Financial authorities and FIs should collaborate to identify and implement mechanisms to proactively share event, vulnerability and incident information amongst financial sector participants to combat situational uncertainty, and pool knowledge in collective defence of the financial sector.

16. **Protect sensitive information**. Financial authorities should implement secure forms of incident information handling to ensure protection of sensitive information at all times.

1. Introduction

Enhancing cyber resilience is a key priority for financial authorities and FIs and has been a key element of the FSB's work programme to promote financial stability. This work has included developing a better understanding of supervisory and regulatory practices around cyber security,[2] creating a common language related to cyber through the development of a Cyber Lexicon[3] and establishing a toolkit of effective practices for cyber incident response and recovery.[4] In many jurisdictions, financial authorities have introduced CIR requirements for FIs, which are crucial for effective policy response and promoting financial stability. Over the last decade however, meaningful differences have and continue to emerge in the requirements and practices associated with CIR, which the FSB explored in greater detail in its 2021 stocktake.[5]

Drawing from a survey of FSB members conducted in early 2022, the FSB identified commonalities in CIR frameworks (detailed in Annex A) and practical issues associated with the collection of cyber incident information from FIs and the onward sharing between financial authorities. Section 2 describes the practical issues, which include: (i) operational challenges arising from the process of reporting to multiple authorities; (ii) setting appropriate and consistent qualitative and quantitative criteria/thresholds for reporting; (iii) establishing an appropriate culture to report incidents in a timely manner; (iv) inconsistent definitions and taxonomy related to cyber security; (v) establishing a secure mechanism to communicate on cyber incidents; and (vi) legal or confidentiality constraints in sharing information with authorities across borders and sectors. Section 3 sets out 16 recommendations to address these practical issues and challenges to achieve greater convergence in CIR. These recommendations were informed by the experiences of financial authorities and engagement with FIs.

2. Practical issues and challenges to achieving greater convergence in CIR

The 2022 survey augmented and refined the stocktake in 2021,[6] delving more deeply into understanding: (i) the most common reporting objectives for financial authorities; (ii) the types of incident reporting used to support common objectives; (iii) impediments to sharing information between financial authorities; (iv) the information items exchanged as part of incident data collections; (v) aspects considered for impact/materiality thresholds that trigger reporting obligations; and (vi) practical issues financial authorities and FIs have in collecting or using the reported cyber information. This work identified many commonalities in CIR frameworks across jurisdictions and sectors. This includes commonalities in reporting objectives, the types of data collected on incidents and the use of criteria or materiality thresholds to trigger FIs' reporting obligations (i.e. institution-initiated reporting). (See Annex A for more analysis of the survey findings.)

---

2 FSB (2017), *Summary Report on Financial Sector Cyber security Regulations, Guidance and Supervisory Practices*, October.

3 FSB (2023).

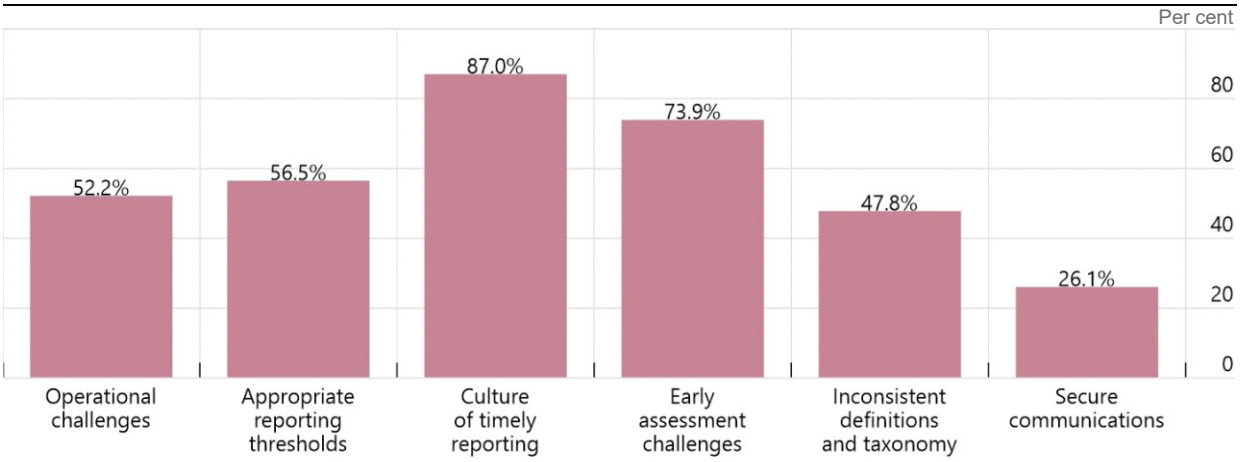
4 FSB (2020), *Effective Practices for Cyber Incident Response and Recovery*, October.

5 FSB (2021), *CIR: Existing Approaches and Next Steps for Broader Convergence*, October.

6 FSB (2021).

The survey also found that differences in reporting requirements can arise due to different policy objectives and mandates, as well as differences in FIs' size, business activities and services. The different reporting requirements, different uses of information and subsequent heterogeneous information can create challenges for both FIs and financial authorities. Graph 1 illustrates the practical issues financial authorities and FIs face when collecting or using reported cyber incident information.[7] These issues are interrelated. For instance, an FI that faces operational challenges in submitting CIR reports may find it more difficult to develop a culture that promotes the timely reporting of cyber incidents. Further, differences in regulatory requirements or reporting of cyber incidents, primarily for FIs that operate in many jurisdictions, could result in operational challenges that again impact the quality and timeliness of reporting.

Practical issues in collecting or using cyber incident information **Graph 1**



Source: 2022 FSB Survey

2.1. Operational challenges

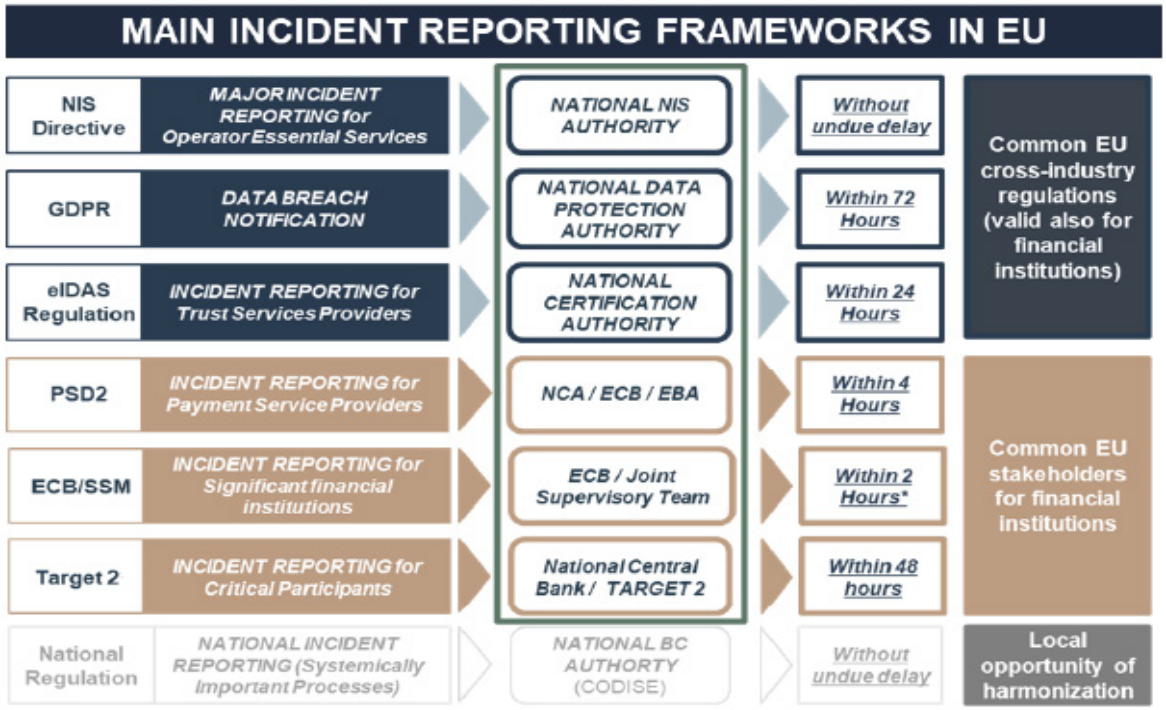
Institution-initiated reporting of cyber incidents by FIs is typically triggered by exceeding implicit or explicit criteria and is normally associated with specific reporting obligations, such as a requirement to submit letters of notification, complete incident templates or report via other online tools/platforms. Meaningful differences in how different authorities determine their reporting criteria for cyber incidents, use incident information and set their timeframes for reporting an incident pose operational challenges for FIs; particularly for FIs that operate across many jurisdictions and sectors and are subject to multiple reporting requirements for one incident, with each report tending to trigger follow-up enquiries from each financial authority. In addition, many FIs are required to report to law enforcement, cyber insurance, industry threat sharing groups, customers and stakeholders within set timeframes, as well as internally to business continuity teams, corporate executives and corporate communication teams. At the same time, incident response teams are working to address the incident, minimise the harm and recover operations as quickly as possible.

Figure 1 illustrates how FIs operating in the European Union (EU) have to report incidents to multiple authorities under different EU regulations/directives and under different timeframes,

[7] Ibid., page 11.

ranging from 'without undue delay' to 'within 72 hours'. The reporting process involves authorities at both the national and European level, often applying different procedures, criteria/thresholds, templates and taxonomy. The newly developed Digital Operational Resilience Act (DORA) is a step towards harmonisation of incident reporting requirements across the EU, paving the way towards a centralised EU incident hub.

Incident Reporting Frameworks in the European Union **Figure 1**



Source: European Banking Federation (2020). *EBF position on CIR*, June.

Figure 2 presents a case study that was developed in collaboration with a global systemically important bank (G-SIB) with large operations in Europe and the United States. In the event of a cyber incident which triggers reporting requirements in all jurisdictions that the G-SIB operates, the G-SIB, in the first 72 hours, has to verbally contact five or more authorities, issue between 7-13 written reports, complete and submit 12-14 initial incident report forms and enter details into 5-9 online reporting portals.[8] Each report is edited and reviewed by incident response teams to ensure it is technically accurate according to the latest information as more details of the incident emerge, which is particularly dynamic in the first 24 hours of an incident. Further, draft text in each required communication format, style and timeframe are iterated and finalised with the most current information available, which takes considerable time away from the relatively small-sized teams of cyber incident responders during most critical initial investigation time.

There are also meaningful differences in the reporting templates and reporting triggers (i.e. detection or materiality thresholds), which require judgement by the G-SIB, and mechanisms for reporting (e.g. verbal, email, template-based, online form). The challenge of

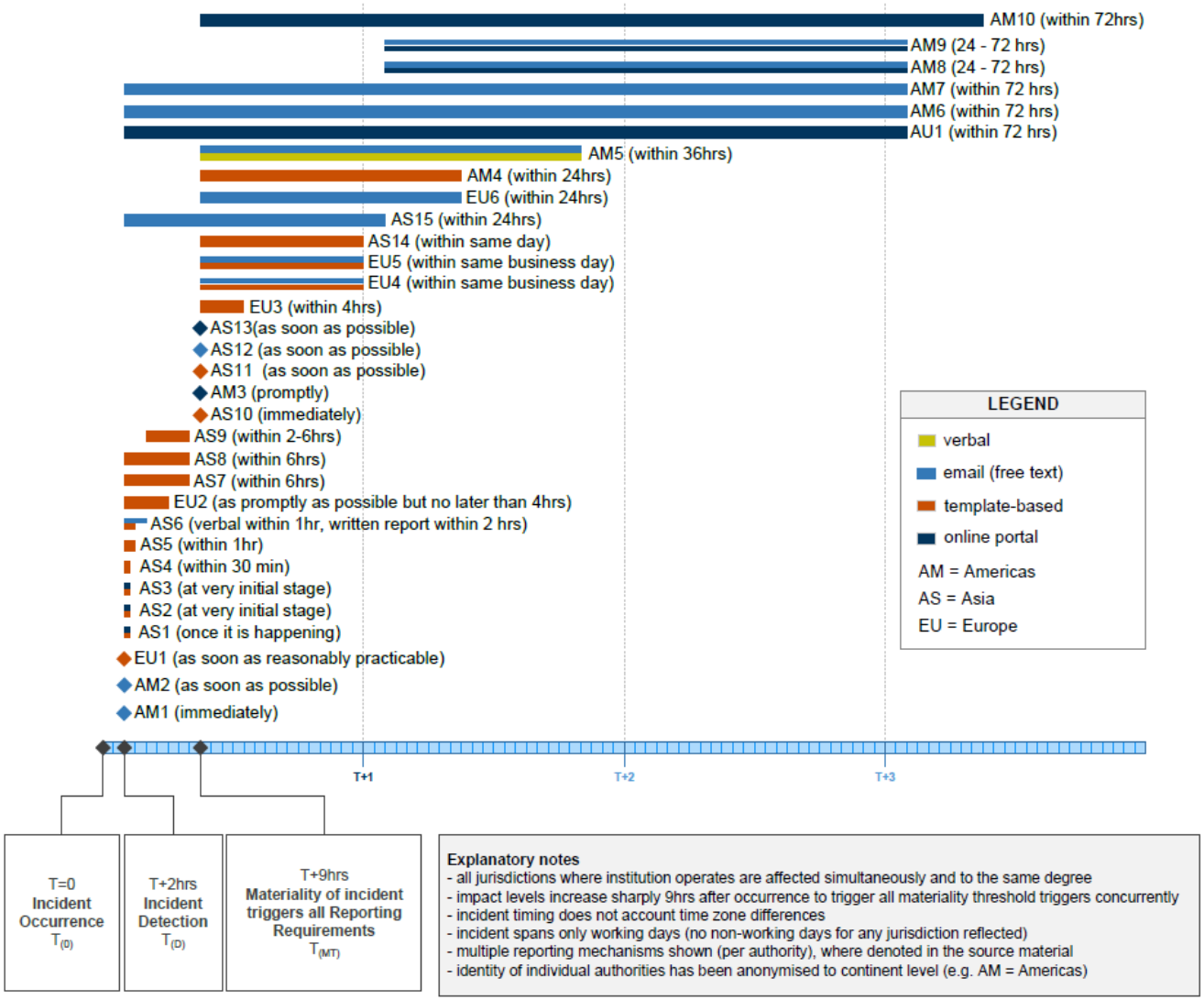
8 Additional layers of complexity would be added if incident reporting to non-financial sector authorities and agencies were included in this case study.

materiality thresholds as triggers for reporting in the first 24 hours is further exacerbated by the uncertainty that surrounds the first hours of an event detection, which has led several financial authorities to issue verbal guidance for proactive reporting of incidents with a potential to be cyber-related, or a potential to be materially impactful but the threshold has not yet been reached. Further, each reporting requirement may have different governance processes, which need to be managed while managing the incident itself.

Finally, in addition to mandatory incident reporting, FIs may need to manage ad-hoc information requests from financial authorities on both cyber incidents and cyber events, which could pose additional demands on the FI's already limited resources.

Illustration of incident reporting requirements for a G-SIB

Figure 2



2.2. Setting reporting criteria

The process of determining and articulating the point at which a reporting obligation becomes actionable following a cyber incident poses challenges for financial authorities, and hinders convergence in CIR.

First, the calibration of reporting criteria can present practical issues, including:

- setting reporting criteria which is cause-agnostic (i.e. relevant in all incident circumstances) and proportionate in nature, and therefore applicable to a diverse range of FIs of differing scales, complexity and types;
- determining an appropriate duration for FIs to fulfil their reporting obligation once it has been triggered;
- for detection-based triggers, balancing the time (on average) that may require FIs to sufficiently understand the nature of an incident before submitting an initial report, against the financial authority's need to be informed in a timely manner; and
- for materiality-based triggers, overcoming the inherent difficulty in describing or measuring impact and severity, given the lack of established methodologies to guide financial authorities[9] and FIs.

Second, there is a potential for a lack of common understanding on reporting criteria between financial authorities and their regulated FIs. This 'interpretation risk' can arise as a result of insufficient detailed criteria, thereby increasing the likelihood of FIs incorrectly or inconsistently executing against authority expectations. Under such circumstances, it is possible that authorities may experience greater levels of under-, over- or late reporting which may in turn affect their ability to fulfil their reporting objectives. On the other hand, trying to define too many criteria can increase operational complexity with reporting.

Third, the calibration of reporting criteria is often specific to each financial authority, thereby limiting convergence opportunities. The point at which an authority wishes to be informed of a cyber incident will be influenced by its institutional mandate, or by cross-sectoral requirements. Figure 2 illustrates this diversity of reporting periods implemented by 32 different authorities for initial reporting by FIs. Convergence is less likely for impediments that are foundational in nature. However, other aspects of reporting criteria which are less driven by mandates (such as intermediate or final reporting) may present opportunities for alignment such that the timing of a subset of incident reports may coincide to be received by multiple authorities simultaneously.

2.3. Culture of timely reporting

Late reporting of cyber incidents by FIs could delay or impede the assessment and responses by financial authorities. The resulting impact could be significant, especially when there are

9 FSB (2021), page 3.

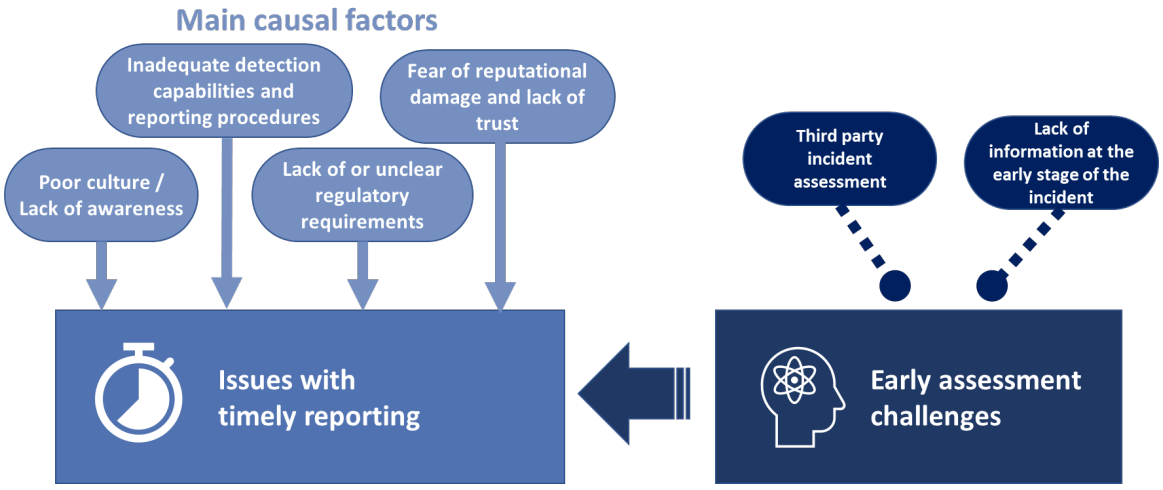
potential sector-wide implications or spill-over effects to other FIs necessitating supportive action from an authority. For example, a widespread incident could quickly escalate into a crisis, and the financial authority may decide to issue media statements to the public to maintain their confidence in the financial system. Effective cyber incident communication can only be achieved when the financial authority has timely and sufficient information relating to the incident. Having timely reporting of such information could also be helpful for cross-border coordination of joint actions and responses.

Establishing an appropriate culture or behaviour among FIs to report cyber incidents in a timely manner remains a challenge, and may require a change in mindset. This may be due to (see Figure 3):

- poor culture or lack of awareness in FIs on the need for timely CIR;
- fear of reputational damage or increased scrutiny from the relevant financial authority;
- delayed detection and assessment of cyber incidents in FIs due to inadequate detection capabilities, increasingly complex IT environments, and/or adoption of new technologies that staff may not be fully familiar with;
- lack of or unclear reporting requirements that may be open to interpretation by FIs or financial authorities;
- inadequate internal escalation and reporting procedures in FIs; or
- a lack of trust on the part of individual employees or organisational units in an FI that may impede the timely escalation of cyber incidents.

At the same time, difficulties in making accurate assessments during the early stage of a cyber incident, including in relation to cyber incidents affecting third-party service providers that do not share timely information with FIs, may also contribute to the issue of late reporting.

Possible causal factors to issues with timely reporting **Figure 3**



2.4. Early assessment challenges

Due to the ambiguous nature of many cyber incidents in general, the true impact or root cause of the incident may not be known for some time. This makes obtaining relevant cyber incident information in the early phases of the incident a challenge, hindering the ability to assess the impact of an incident. This creates challenges for authorities to coordinate and communicate relevant responses in a timely manner to ensure stability of the financial system. Information often is not communicated in a standard way and different authorities may receive different amounts of information at different times, impacting the ability for authorities to come up with a common operating picture and cohesive policy response. A timely and clear picture of an incident is important for financial authorities as it forms the basis for any policy response; including supervisory responses or in the case of a more material incident, public communication or tools to address potential systemic impacts.

The challenge for FIs is that some cyber incidents are often not easy or straightforward to identify. Detection of an incident may lag significantly after the first occurrence and the extent of the impact may not be obvious at first (e.g. if there is no service down time). Assessing the full extent of the impact of cyber incidents can take a long time and therefore may continue beyond the initial thresholds and reporting requirements. Expectations to complete this type of assessment for reporting purposes early on, while important, add additional stress and diverts resources from focusing on resolving the incident. The resources to analyse the root cause of an incident will vary depending on the complexity of the incident. In the case of an incident initiated for malicious purposes, the instigating party may take steps to obfuscate impact.

The lack of sufficiently skilled and experienced cyber professionals could also impact an FI's ability to identify and assess the situation in a timely manner. Challenges may be exacerbated at small institutions, which may lack resources for continuous monitoring, automated detection and forensic analysis. On the other hand, large FIs experience a higher volume of cyber incidents, many of which may not be noteworthy for the institution or its financial authorities.

2.5. Secure communications

Information contained within incident reports can be both commercially and market sensitive, and therefore needs to be handled appropriately by all parties involved. The diverse nature of reporting mechanisms used by authorities presents operational challenges, as highlighted in Section 2.1. From a security perspective, FIs need to ensure that they can meet these varied requirements at all times. From an FI perspective, there may be insufficient clarity or confirmation that certain authority reporting platforms meet shared security requirements, thereby exposing FIs to potential sources of risk, particularly as unencrypted e-mail is the most common way FIs report a cyber incident.[10] FIs may also have concerns about reporting platforms being actively targeted by threat actors.

[10] FSB (2021), page 7.

2.6. Cross-border and cross-sectoral issues

While many financial authorities have formal or informal information-sharing arrangements with authorities outside their jurisdiction,[11] there are differences in the scope, depth and form of such information-sharing across jurisdictions and sectors. Through the FSB survey, two themes emerged as impediments to information sharing across borders and sectors:

- legal, whether the pre-requisite laws or agreements are in place to set out the terms by which incident information can be shared between parties; and
- confidentiality, i.e. the treatment/handling of protected information between parties.

In the majority of cases, as long as agreements are in place, such as Memoranda of Understanding (MoUs) or legal gateways, and the information transferred does not breach the terms of what can be exchanged, then fewer impediments are observed.

Cross-border arrangements are 'appetite-driven', governed by individual authorities' desires to share with other parties and to what extent as well as historical experience. In most circumstances, financial authorities prefer to enter into bilateral agreements with one another, resulting in a patchwork of idiosyncratic engagements which, whilst perhaps not being the efficient outcome, reflect the nature/closeness of relationships. Although multilateral arrangements do exist, these tend to align to pre-defined circles of trust.

3. Recommendations

Drawing from the FSB's body of work on cyber, including engagement with external stakeholders, this report sets out recommendations to address impediments to achieving greater convergence in CIR.[12] The recommendations aim to promote convergence among CIR frameworks, while recognising that a one-size-fits-all approach is not feasible or preferable. Financial authorities and institutions can choose to adopt these recommendations as appropriate and relevant, consistent with their legal and regulatory framework.

3.1. Design of approach to CIR

Recommendation 1. Establish and maintain objectives for CIR

Financial authorities should have clearly defined objectives for incident reporting, and periodically assess and demonstrate how these objectives can be achieved in an efficient manner, both for FIs and authorities.

Financial authorities should review the coverage and appropriateness of the five commonly identified reporting objectives (See Annex A) within their CIR regime. In some cases, a financial

[11] Authorities may also have information-sharing arrangements with cyber security or data privacy agencies within the same jurisdiction.

[12] Annex B highlights the many-to-many relationships between the recommendations and the practical issues they seek to address, and the extent to which each recommendation is projected to have a positive impact.

authority's CIR objectives may be implicitly contained within broader objectives related to incident reporting, which may be inclusive of, rather than exclusive to, cyber incidents. When defining objectives, financial authorities should, where possible, address commonly identified practical issues and impediments associated with CIR (e.g. reduction in operational challenges). Financial authorities should review their CIR objectives at regular intervals to verify that they remain fit for purpose and are proportionate, and ensure that the information sought in the incident reporting continue to meet the needs of all relevant stakeholders. Financial authorities could also engage FIs to clarify their CIR policy objectives, so that FIs can understand and support those objectives.

Recommendation 2. Explore greater convergence of CIR frameworks

Financial authorities should continue to explore ways to align their CIR regimes with other relevant authorities, on a cross-border and cross-sectoral basis, to minimise potential fragmentation and improve interoperability.

Establishing a greater degree of convergence amongst financial authorities will facilitate an easier exchange of information at critical points and promote greater efficiency of CIR requirements for globally active FIs, thereby promoting financial stability. Such alignment could accommodate specific authorities' cross-border and cross-sectoral information-sharing needs.

In jurisdictions where more than one financial authority is designated to receive cyber incident reports, and where operational circumstances and legal frameworks would permit such streamlining, authorities should explore ways to consolidate overlapping CIR processes. Potential approaches include implementing unified CIR to all relevant authorities or designating a lead reporting authority to receive incident reports and disseminate this information to other authorities as appropriate. Authorities in such cases should seek to use common reporting formats for the dissemination of information, which can additionally support the delivery of individual report instances to multiple authority recipients.

Financial authorities should also explore alignment of mechanisms for secure exchange of incident reporting information, including opportunities to harmonise reporting channels with other financial authorities that receive CIR information.

Recommendation 3. Adopt common data requirements and reporting formats

Financial authorities should individually or collectively identify common data requirements, and, where appropriate, develop or adopt standardised formats for the exchange of incident reporting information.

The adoption of common data requirements and reporting formats can occur at three different scales that build incrementally in terms of scope, complexity and ambition (outlined below). Financial authorities should determine the level of adoption, which is appropriate to their circumstances, noting that any change in reporting formats would likely have implementation implications for affected FIs in scope. Financial authorities are encouraged to engage with FIs to inform the development of their CIR data requirements and reporting formats. Common approaches could contribute to fostering trust and collaboration and may be adopted:

- By a single authority, where reporting requirements are not currently explicitly defined. In such cases, FIs would have a high degree of flexibility, but might lack the necessary clarity to provide the financial authority with incident information in a consistent manner. Defining formats for individual data fields within incident reports may realise further benefits related to the exchange and processing of the reported information. In the absence of central guidance, individual supervisors may resort to agreeing these requirements on a bilateral basis with FIs, which in turn could be less efficient for authorities, and may hamper the ability to conduct horizontal analysis.

- By financial authorities within the same jurisdiction. Adoption of a common reporting format by financial authorities within a single jurisdiction can provide a more efficient solution for reporting requirements originating from that jurisdiction. This change can be particularly helpful for FIs that are solely domestically regulated.

- By (a subset of) financial authorities across jurisdictions. Adoption of a common reporting format across borders could benefit FIs with a global footprint. In addition, broader adoption of a common format can drive efficiencies for the cross-border exchange of incident information between financial authorities in a standardised form.

Financial authorities may also consider accepting the format and content of a cyber incident report that FIs must submit to their main supervisory or oversight authority.

Recommendation 4. Implement phased and incremental reporting requirements

Financial authorities should implement incremental reporting requirements in a phased manner, balancing the authority's need for timely reporting with the affected institution's primary objective of bringing the incident under control.

Initial cyber incident reports[13] should aim to contain a minimal set of information items which may then be supplemented by more comprehensive intermediate updates and culminate in a final report which also includes the post-incident analysis performed by the impacted FI.

In the early stages of a cyber incident, confidence levels on causes and circumstances of the incident may be low and the impacted FI may not have a comprehensive understanding of the event that has occurred. At the outset of the incident, the situation could be unstable and may continue to evolve. At the same time, the resources and efforts of the impacted FI are primarily focused on incident response and impact containment. Therefore, initial reporting requirements should be constrained to facilitate timely reporting and not compound the operational challenges which the affected institution already faces.

As the FI gains better clarity and obtains more details over the course of its incident management, it can then provide further updates through intermediate or final reporting (as the case may warrant) to the financial authority. To ensure proper closure after the incident has been resolved, the final reporting should cover the FI's root cause analysis and after-action review.

---

[13] In some jurisdictions, mandatory initial reporting requirement for CIR purposes may be referred to, or be synonymous with the term "notifications". In others, "notification" refers to a separate and distinct process from CIR and involves the early/informal alerting of incidents to authorities prior or separate from a mandatory reporting requirement. To avoid confusion, this report uses the generic term "initial reporting" except when referring to jurisdiction-specific requirements.

Box 1: Examples of information that could be reported to authorities in each CIR phase

Starting from a minimum set of information to be provided in the initial reporting, FIs can provide more details as they become known/available during the subsequent phases of the CIR process, as outlined below.

Initial reporting

In the early stage of the incident, the information available to the affected FI could be rather limited. Nevertheless, the FI should still provide, to the best of its knowledge, an overview of what happened, which could include when the incident was detected, possible cause(s) of the incident, immediate impact (e.g. the services affected) and initial actions taken to manage the incident. Such information could help authorities form a preliminary assessment on the severity of the incident, as well as any potential spill-overs on other entities and the financial system as a whole. The contact information of person(s) designated as the point of contact(s) for the incident should also be provided to facilitate any follow-up communications required.

Intermediate reporting up until (and including) incident resolution

As the incident evolves, more details would become available to the FI. Updates may be provided on the latest impact observed (e.g. operational, financial and reputational impact), including the systems and services affected, and the technical details about the incident. Other useful information may include escalation steps taken, response and recovery actions to restore services, stakeholder's engagement and further insights on incident causes. These intermediate report(s) would provide financial authorities with a better picture of the latest developments and potential implications arising from the incident.

Final reporting

Following the incident, the FI may be required to report on its after-action review and root cause analysis. Useful information may include main findings and learning points, and remedial activity. With the final report, the authorities become aware of how the incident originated, the level of preparedness, response and recovery of the affected entity, as well as the actions and measures to prevent similar incidents in the future.

Recommendation 5. Select appropriate incident reporting triggers

Financial authorities should explore the benefits and implications of a range of reporting trigger options as part of the design of their CIR regime.

For each reporting type[14], the process for determining the reporting trigger should aim for outcomes which are proportionate, comprehensible and justifiable. For each reporting type, financial authorities may select from a range of different trigger options which affect the timing and/or timeframe for reporting.

- For institution-initiated reporting, the primary design choice is whether to anchor reporting requirements relative to (1) incident occurrence or detection, or (2) when a financial institution assesses an incident to meet a pre-defined materiality threshold(s). Common materiality thresholds include quantitative measures based on service downtime, impact to profitability or customers, though these have to be scaled or

[14] Refer to Annex A, Section 2 for the definitions of the different reporting types.

implemented relative to financial institution size. Materiality thresholds can also be qualitative, like based on reputational impact. Factors such as ease of understanding, scenario independence, situational uncertainty and institutional decision-making should be considered as part of trigger evaluation.[15]

- For authority-initiated reporting, financial authorities should consider the circumstances and the process required to trigger sectoral impact assessments, on either a national or cross-border basis.

Authorities may also collect cyber incident data on a periodic basis. As the trigger for periodic reporting is time rather than event driven, financial authorities should consider the frequency of data collection relative to the volume of incident information collected for the chosen reporting period. Authorities may opt for a uniform interval across their regulated institutions, or vary frequency in accordance with firm type, scale and complexity. The relative timing of bulk data collections from all institutions in scope may be either: aligned, though this may present challenges in handling the aggregate volume of information received concurrently; or spread out such that individual institutions report on their own periodic cycles, which could introduce additional complexity to external messaging.

Box 2: Examples of reporting triggers

In the **United States**, the Federal Banking Agencies notification rule requires a banking organisation to notify its primary federal regulator of any 'computer-security incident' that rises to the level of a 'notification incident', as soon as possible and no later than 36 hours after the banking organisation determines that a notification incident has occurred based on defined qualitative criteria that requires the bank's judgement that those criteria have been met. In addition, the Securities Exchange Commission (SEC) Regulation Systems Compliance and Integrity (SCI) requires designated SCI entities to notify the SEC of any 'SCI event' (including systems intrusions, disruptions and compliance issues) immediately upon responsible SCI personnel having a reasonable basis to conclude that an SCI event has occurred. Within 24 hours, SCI entities must submit a written notification of the event to the SEC, including certain prescribed information.

The **European Union** follows the Payment Services Directive (PSD2) reporting scheme, in some instances, and requires institutions to classify major incidents based on fulfilling one or more criteria at a defined 'Higher impact level', or three or more criteria at the defined 'Lower impact level'. Examples provided include:

- More than 5,000 or 10% of payment services customers is considered a lower impact level, while more than 50,000 or 25% of payment services customers is considered a higher impact level.
- An economic impact greater than the maximum of 0.1% Tier 1 capital or greater than €200,000, or greater than €5 million is considered a higher impact level.
- More than 10% of an institution's regular level of transactions (in terms of number of transactions) and €500,000 is considered a lower-level impact.
- More than 25% of an institution's regular level of transactions (in terms of number of transactions) or greater than €15 million is considered a higher impact level.

[15] See Annex A, Section 3 for more details about the considerations to take into account when selecting the reporting triggers.

Recommendation 6. Calibrate initial reporting windows

Financial authorities should consider potential outcomes associated with window design or calibration used for initial reporting.

When setting initial reporting windows, financial authorities should consider a range of factors including: (i) the window type i.e. whether the window is start-bound, end-bound or uses a defined window; (ii) language choice, which can convey different emphasis; and (iii) the size of the window, which may be influenced by the reporting trigger type. The reporting windows should be carefully calibrated in order not to put additional strain on FIs in responding to the cyber incidents.

Where reporting triggers are time-driven (i.e. occurrence or detection), longer windows could be implemented to allow sufficient time for FIs to reasonably assess the nature of the incident. Conversely, where materiality thresholds are used, FIs should have already partially assessed the nature of an incident, and therefore shorter reporting windows could be implemented such that authorities can be rapidly informed and act accordingly. When determining the reporting windows, financial authorities should also ensure that the merits of early reporting are suitably taken into account, while balancing against the quality and completeness of the information that can reasonably be gathered during the timeframe. As covered under Recommendation 4, phased reporting is one way to balance the operational burden on FIs who may not have complete information about an incident at the outset, while ensuring financial authorities are informed and prepared to respond as early as practicable.

Recommendation 7. Provide sufficient details to minimise interpretation risk

Financial authorities should promote consistent understanding and minimise interpretation risk by providing an appropriate level of detail in setting reporting thresholds, using common terminologies and supplementing CIR guidance with examples.

Financial authorities should consider approaches to minimise interpretation risk (i.e. a misalignment of authority expectations versus institution understanding) through clarity of expression and illustrating intent behind policy or rulemaking for CIR thresholds. Authorities should also consider leveraging common terminologies, which will be particularly valuable for FIs subject to multiple reporting requirements and potentially conflicting terminology.[16] Irrespective of whether an authority takes a qualitative, quantitative or blended approach to defining its reporting criteria, the level of detail provided should seek to be as informative as possible, whilst being mindful of introducing undue complexity.

Box 3: Examples of Incident Reporting Guidelines

Hong Kong Monetary Authority (HKMA)

The HKMA expects authorised institutions (AIs) to report all significant operational incidents (including cyber incidents) to the HKMA. As the nature of every operational incident is different, the HKMA does not prescribe set thresholds that apply across-the-board to all AIs, but rather, expects individual AIs to

[16] Common terminology includes the FSB's Cyber Lexicon, and/or terminology produced by international and domestic standard development organizations such as the International Organization for Standardization (ISO).

exercise their judgement and establish internal guidelines for determining the materiality of incidents based on their own circumstances and risk profile.

To reduce AIs' reporting burden and enable them to devote resources to handling the more significant incidents, the HKMA has issued guidance to help AIs better understand the types of incidents that it expects to be reported. Therein, the HKMA articulates: (i) factors that AIs should assess in determining whether an incident is significant (e.g. risks of data leakage, financial and reputational implications, the impact on services and customers), (ii) examples of incidents that the HKMA would generally consider to be significant and require reporting, as well as (iii) examples of incidents that would generally not require reporting. With respect to cyber incidents, specifically, the HKMA notes, for instance, that those involving attacks on an AI's wholesale payment instructions (regardless of whether the attacks are successful) or e-banking services (with successful log-ins to customer accounts or resulting in unauthorised transactions), and cyber extortion targeting at an AI would generally be considered as significant and require reporting.

In addition to the guidance on incident reporting, the HKMA also issues email alerts from time-to-time to keep AIs updated on severe risks and threats that may be emerging in the cyber landscape. Besides raising AIs' awareness and preparedness for these potential risks, the alerts also serve to reinforce the HKMA's view that significant cyber incidents would warrant reporting if encountered.

Reserve Bank of India (RBI)

The RBI has a dedicated web portal where the Regulated Entities (REs) report unusual cyber security incidents as well as certain incidents of significant nature (even if those are not necessarily associated with cyber medium) within 2-6 hours of detection. The portal, through a workflow system, enables the REs to report the incident with necessary details/documents and the RBI to review the response and action taken until the incident is treated as closed. The portal, apart from the incident details, captures impact assessment, stakeholder communication, root cause analysis, IOC details, recovery mechanism and the RBI's assessment of the incident.

Incidents that compromise or attempt to compromise the confidentiality, integrity or availability of REs' information that are stored/processed in the information assets of the RE and/or its third-party service providers (TPSPs) are required to be reported. For example, it includes malware/ransomware attacks; data/business information loss, leakage and compromise; DoS/DDoS attack; email spoofing and attacks. Other types of incidents that are required to be reported include: breaches in thresholds of customer service disruptions due to non-availability of IT systems, as well as breaches in thresholds of 'significant' loss due to phishing/vishing attacks on customer(s). While reporting the incident, REs are required to provide attack pattern (e.g. common attack pattern enumeration and classification (CAPEC-ID)) wherever relevant.

Recommendation 8. Promote timely reporting under materiality-based triggers

Financial authorities that use materiality thresholds should consider fine-tuning threshold language, or explore other suitable approaches, to encourage prompt reporting by FIs for material incidents.

FIs require time to perform analysis on whether materiality thresholds have been breached, but need not wait for absolute certainty to report. In certain cases, FIs may have information that strongly suggests that a materiality threshold will reasonably likely be breached before that occurs. Based on the initial incident details available, which may be somewhat limited, financial authorities should encourage FIs to take a forward-looking approach to their assessment and determination of what incidents would warrant reporting. Such an approach would help financial

authorities to be aware of issues that are likely to become material as early as possible and take any action as appropriate. The FI may be able to immediately determine that the incident is unlikely to be resolved before the threshold will be breached. Accordingly, the FI could begin the process to alert authorities earlier than the latest period required.

As the FI continues to assess the impact, the FI should be able to confirm or "downgrade" the incident as warranted (i.e., informing the authorities that the FI no longer believes the incident to meet the reporting threshold.)

3.2. Supervisory activities and collaboration between authorities

Recommendation 9. Review the effectiveness of CIR and cyber incident response and recovery (CIRR) processes

Financial authorities should explore ways to review the effectiveness of FIs' CIR and CIRR processes and procedures as part of their existing supervisory or regulatory engagement.

Reviews of FIs' CIR processes and procedures may identify potential gaps that could lead to under-, over- or late reporting. Where possible, financial authorities could perform such reviews within their ongoing supervision by including, inter alia:

- drills and thematic assessments to evaluate FIs' plans and procedures to achieve the required levels of CIR (e.g. standard operating procedure for communication and coordination, clear reporting standards);
- on-site inspections or independent reviews (e.g. comparing internally logged incidents with notified incidents to the authority, adequate cyber incident response tools);
- collecting information on cyber incidents from other information sources (e.g. cyber incident reports from other FIs, third parties or other sectors; media reports; other information sharing arrangements).

Cyber security tests and exercises carried out by FIs could also include CIR plans and procedures in order to seek a continuous improvement of their internal capabilities based on the lessons learnt. FIs could also engage an independent party to assess their incident management measures and processes, including procedures for incident escalation and reporting.

Additionally, the process for reporting an incident begins before an incident occurs and are often influenced by elements of an institution's CIRR program and processes. Therefore, there may also be merits for financial authorities to review these capabilities as part of their supervisory engagement, which could result in better CIR outcomes.

Recommendation 10. Conduct ad-hoc data collection

Financial authorities should explore ways to complement CIR frameworks with supervisory measures as needed and engage FIs on cyber incidents, both during and outside of live incidents.

Financial authorities may use their supervisory toolkit to enhance information collection regarding cyber incidents beyond any specific reporting requirements.

Potential situations that could warrant the use of the supervisory toolkit include:

- A financial authority receives limited information about a severe cyber incident warranting continuous monitoring.
- A financial authority receives information about a cyber incident at one institution, which has the potential to be replicated at other institutions.
- A financial authority receives information (e.g. perhaps through press reports or other government channels) regarding a potential vulnerability or cyber event and seeks to minimise impact on regulated FIs.

The use of the supervisory toolkit in this situation, like in others, depends on supervisory judgement and the specific facts and circumstances around a cyber incident, and the limited information that supervisors may have at any point in time. Financial authorities should, where circumstances allow, consider ways to increase cross-border and cross-sectoral cooperation with respect to FIs that are subject to multiple regulations.

Recommendation 11. Address impediments to cross-border information sharing

Financial authorities should explore methods for collaboratively addressing legal or confidentiality challenges relating to the exchange of CIR information on a cross-border basis.

Financial authorities can use MoUs, or other equivalent arrangements, to outline the basis for the information exchange between authorities, which typically include commitments to maintain the confidentiality of information. However, in some cases, existing arrangements may not clearly cover the sharing of information related to cyber issues and incident reporting, or sufficiently address issues that may prevent these exchanges from taking place. Financial authorities should consider whether the collaborative development of model clauses can enhance such MoUs and information exchanges.

To further improve cross-border cooperation, financial authorities should explore the benefits and applicability of regional or global reporting frameworks. Cross-border arrangements such as the European Central Bank Single Supervisory Mechanism (ECB SSM) and European Banking Authority (EBA) reporting frameworks in the EU, Gulf countries cooperation agreement, and DTN-CRISP demonstrate the benefits for participants, irrespective of which framework is used.

In addition, financial authorities can take steps to avoid inclusion of protected information unless able to satisfy relevant data protection legislation across jurisdictions involved. In most cases,

that level of detail would only be required if exchanging information on the technical response to the incident.

Box 4: Monetary Authority of Singapore's (MAS) bilateral information-sharing arrangements with other financial authorities

- Arising from discussions at the FSB, MAS and HKMA embarked on a pilot arrangement to share cyber security information in 2017. Both authorities had since established a set of terms of reference that laid out the governance arrangement, guiding principles, scope, modality and approach for bilateral information sharing.
- Further to that, MAS has also established cyber security cooperation MoUs separately with the US Treasury, French financial authorities (Banque de France (BdF), Authorité de contrôle prudential et de resolution (ACPR)) and UK financial authorities (HM Treasury, Bank of England (BoE), Financial Conduct Authority (FCA)) to facilitate bilateral cyber information exchange and collaboration in areas, such as conduct of joint cross-border exercises.
- The MoUs and written agreements for these bilateral information-sharing arrangements contain clauses that dictate the protocols and measures for the parties to properly handle and protect the information shared. There are also clauses that define specific circumstances and types of information where written consent needs to be sought for onward sharing.
- It is common to use a Traffic Light Protocol ('TLP') for the sharing authority to indicate with whom and how the information may be shared by the receiving authority. The TLP terms could be tailored to meet the needs and intentions of the authorities, reducing the impediments to information sharing.

3.3. Industry engagement

Recommendation 12. Foster mutual understanding of benefits of reporting

Financial authorities should engage regularly with FIs to raise awareness of the value and importance of incident reporting, understand possible challenges faced by FIs and identify approaches to overcome them when warranted.

Continuous engagement between financial authorities and FIs may help to develop a common understanding with regards to the framework and criteria for CIR, including CIR policy objectives. Discussions may also cover the legal and technical measures in place to protect information that is reported to financial authorities, including how and under what circumstances this incident information may be further shared. Financial authorities should consider periodically reviewing their CIR requirements and processes and incorporating feedback from FIs as appropriate. Such engagements could take place in the form of industry workshops and seminars, or dialogues with industry associations and FIs. Finally, sharing findings (in an aggregated and anonymised way) on cyber incident reports, i.e. on sectoral incident trends, could provide a beneficial feedback loop to FIs.

Recommendation 13. Provide guidance on effective CIR communication

Financial authorities should explore ways to develop, or foster development of, toolkits and guidelines to promote effective communication practices in cyber incident reports.

FIs may benefit from further guidance from authorities on effective practices in terms of the different types of reports associated with specific cyber incidents. Guidance could help improve the clarity of initial reporting. Guidance could also help standardise the quality of interim and final reporting when the reporting institution has more information (e.g. whether to include indicators of compromise or other more detailed information).

3.4. Capability development (individual and shared)

Recommendation 14. Maintain response capabilities which support CIR

FIs should continuously identify and address any gaps in their cyber incident response capabilities which directly support CIR, including incident detection, assessment and training on a continuous basis.

To encourage preparation around incident detection and reporting, FIs should consider adopting effective practices, such as those outlined in the FSB's toolkit of Effective Practices for Cyber Incident Response and Recovery (see Box 5).[17] In many cases, the FSB toolkit recognises that certain specialised incident response and reporting capabilities may not always be retained in-house, particularly for smaller institutions, and can be obtained from third-parties or affiliated organisations. In particular, vendors or external consultants can help with technology solutions, security monitoring, forensic capabilities and trusted information resources to provide additional capabilities to a FI prior to an incident, and can be rapidly escalated in the response to more complex incidents. Because incidents can manifest because of third-party relationships, FIs should evaluate the need, and ability, to obtain relevant information from third-party providers for a relevant incident report (e.g. through contracts or service-level agreements.) Where appropriate, FIs should encourage their third-party providers to share incident information that impact their provided services. This would facilitate FIs' early assessment of the cyber incidents, as well as response and recovery activities.

Box 5: Relevant practices from the FSB CIRR Toolkit

- **8. Metrics**: Organisations establish metrics to measure the impact of a cyber incident and to report to management the performance of CIRR activities. Metrics can be used to determine the severity or priority of an incident. The severity level will inform how quickly the incident needs to be handled and to whom it might be escalated.
- **9. Resources**: Organisations ensure that CIRR functions are adequately staffed and competencies of relevant personnel are maintained and regularly enhanced.
- **13. Scenario planning and stress testing**: Organisations' plans and playbooks include severe but plausible cyber scenarios and stress tests.

[17] FSB (2020).

- **15. Security operations centre (SOC)**: Depending on their size, complexity and risks, organisations operate a 24x7 SOC or engage third-party security services to meet the needs of the organisation to detect, identify, investigate and respond to cyber incidents that could impact the organisation's infrastructure, services and customers. Various tools, including machine learning, are used for vulnerability management and compliance monitoring to enhance the effectiveness of cyber incident analysis.
- **17. Log management and forensic capabilities**: Organisations develop an effective log management and retention framework that is comprised of tools to manage, collect and store system logs that would be required to facilitate incident investigation and analysis. The types of logs to be collected and retention period of logs could be pre-determined based on supervisory rulemaking, law or the importance of the business data held or transported through the system. Organisations establish technical and forensic capabilities to preserve evidence and analyse control failures, identify security issues and other causes related to a cyber incident. If the organisation does not have its own forensic capabilities, contractual agreements with third-party service providers are established (e.g. forensic retainer services) to support extended cyber forensic investigations, which are immediately activated when needed.
- **18. Technology solutions and vendors**: Organisations implement technologies to enforce their policies and procedures. Organisations proactively acquire third-party services if necessary to augment their in-house CIRR capabilities.
- **19. Third-party service providers.** Organisations maintain a record of third-party service agreements detailing important information such as the scope of the service, the service provider contact information, service validity period and service levels. This is achieved through Service Level Agreements (SLAs) with Key Performance Indicators (KPIs), RPOs, and RTOs as part of the contract with the third-party service provider to guarantee adequate response during cyber incidents. Organisations look through SLAs that rely on subcontractors (e.g. nth parties) and ensure they have protections in place. Organisations pre-designate a primary and an alternate service provider in the event that the former is unavailable to provide immediate support, especially in the case of a system-wide cyber incident. Organisations assess the service delivery capacity of their third-party service providers from the beginning and on an ongoing basis. This practice may prove useful in the case of a system-wide cyber incident where a service provider may not be able to conduct a service with sufficient capacity to support all its clients. Organisations monitor, manage and mitigate cyber risks stemming from third-party service providers through a variety of third-party risk management arrangements.
- **23. Trusted information sources**: Organisations correlate a variety of internal and external information sources for quick threat assessment and root cause analysis of the cyber incident.

Recommendation 15. Pool knowledge to identify related cyber events and cyber incidents

Financial authorities and FIs should collaborate to identify and implement mechanisms to proactively share event, vulnerability and incident information amongst financial sector participants to combat situational uncertainty, and pool knowledge in collective defence of the financial sector.

Where appropriate, financial authorities should consider their role in establishing the collaborative environment to foster new, or enhance existing, information sharing mechanisms for cyber incidents within and across jurisdictions. Under such arrangements, affected institutions may leverage the collective knowledge and capabilities of other FIs to help contain

and resolve live incidents, and reciprocally provide crucial insight to avoid future occurrences or limit the spread to other parts of the financial sector. Financial authorities can also leverage these mechanisms to provide a feedback loop to FIs to enhance cyber resilience across the financial sector, build trust with FIs and encourage a constructive approach to exchanging incident information.[18]

Box 6: Swiss Financial Sector Cybersecurity Centre (Swiss FS-CSC)

- The Swiss Financial Sector Cybersecurity Centre (Swiss FS-CSC) association was founded in April 2022. Like similar organisations worldwide, the association aims to strengthen cooperation between FIs and authorities in the fight against cyber threats, and to increase the resilience of the financial sector. In particular, it aims to facilitate the exchange of information between financial market players and improve cooperation with regard to sector-wide preventive measures and the management of systemic crises. Among the more than 80 founding members are associations, banks and insurance companies, and the Swiss National Bank. Membership of the Swiss FS-CSC association is open to all banks, insurance companies, financial market infrastructures and financial associations that have their registered office in Switzerland and have been authorised by the Swiss Financial Market Supervisory Authority (FINMA), as well as subsidiaries and branches of foreign banks and insurance companies with FINMA authorisation.
- At the Swiss FS-CSC, institutions can pool knowledge in regarding policies and practices for cyber incident response and crisis management, as well as share information on ongoing cyber incidents and threats on a real-time basis.
- FINMA, the National Cyber Security Centre and the State Secretariat for International Finance support it as affiliates.

Recommendation 16. Protect sensitive information

Financial authorities should implement secure forms of incident information handling to ensure protection of sensitive information at all times.

Financial authorities should regularly verify that the mechanisms used to collect, process and store CIR information maintain an appropriate level of security across the different phases/activities (e.g. collection, usage, sharing, disposal) and that sensitive information is handled in line with common security practices, and relevant financial authorities' legal obligations. Financial authorities may also consider relevant security risks in their mechanisms used to collect incident information.

Mechanisms include the use of secured platforms, portals or channels; certified email accounts; or encryption protocols and other technical measures, to protect information both at rest and in transit. In addition, to enhance the reliability of the reporting process, financial authorities should consider establishing back-up communication channel(s) as appropriate, to cover situations where the primary channel becomes unavailable or unusable by the reporting institutions.

[18] Examples of existing private sector collaboration include bodies such as the Financial Services Information Sharing and Analysis Center (FS-ISAC), the Financial Services Cyber coordination Centre (FSCCC) in the United Kingdom, Financial Services Cyber Security Centre (FS-CSC in Switzerland and the Cyber Information and Intelligence Sharing Initiative (CIISI-IE) in Ireland, the Association of Banks in Singapore Standing Committee on Cyber Security (ABS SCCS), or national peer-to-peer groups.

Annex A: 2022 Survey findings

This annex summarises the findings drawn from the responses received on the survey conducted in February 2022 related to financial authorities' reporting objectives, types of reporting and reporting criteria.

1. Reporting objectives

Financial authorities use information from cyber incidents for different purposes depending on, for instance, their respective mandates. From an initial set of 10 unique responses, the list was further consolidated to six reporting objectives as follows:

A. To support **management of the impacts** arising from a cyber incident at one or more institutions (87%)

B. To play an active role in the **technical resolution** of a cyber incident at one or more institutions (13%)

C. To build understanding and/or support **coordination of sector-wide** cyber incidents (96%)

D. To **inform supervisory understanding** of the risk profile and/or capabilities at affected institutions (83%)

E. To **identify potential weaknesses or areas for improvement** in current regulation or requirements (78%)

F. To provide a **consolidated source** of incident data, trends, threats and/or risks across peer firms or the financial sector as a whole (87%)

The survey responses indicated a high degree of prevalence for five of the six identified incident reporting objectives. With one exception, financial authorities that responded to the survey do not engage in the technical resolution of incidents (two responses in this category from national cyber security authorities were also discounted). This objective has however been kept to highlight that the majority of financial authority mandates do not extend to technical resolution.

The four remaining objectives reported, but not taken forward, were:

- *compliance with regulatory requirements*, which was considered intrinsic to the act of reporting;
- *reporting to national authorities*, which was deemed to be a requirement outside of the financial authority scope;
- *data repository to support underwriting*, which was incorporated into Objective F; and
- *as part of Suspicious Activity Reporting (SAR)*, which described another channel for the flow of incident information rather than an objective.

2. Reporting types

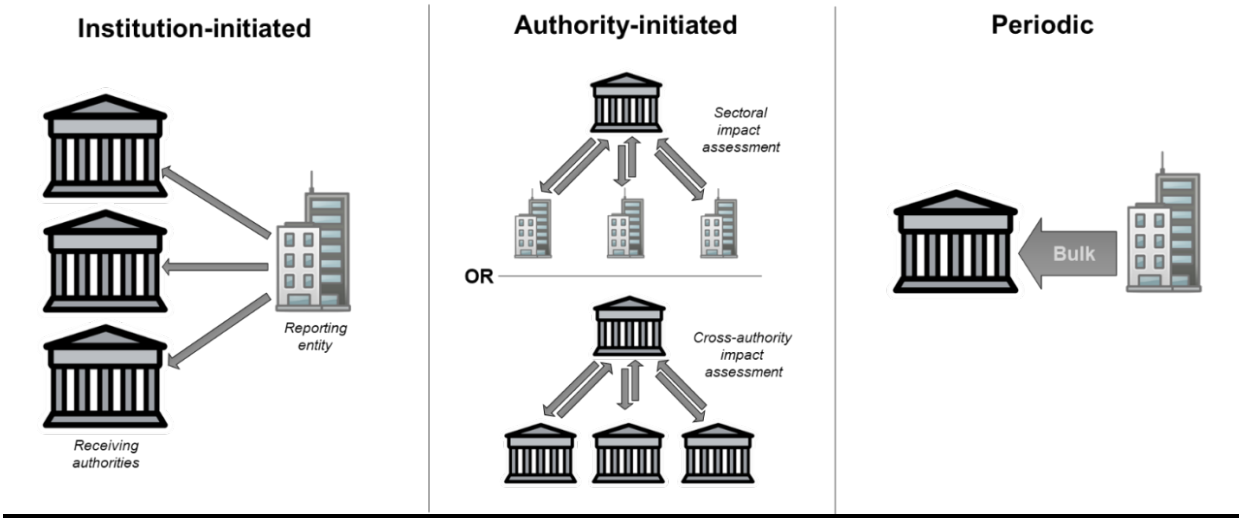
To better understand the types of information flows involved in CIR, the survey explored three types of incident reporting (see Figure 6):

1. **Institution-initiated reporting**, where impacts arising from an incident trigger reporting obligations to one or more financial authorities (and requirement for initial reporting), followed by subsequent intermediate and final reports.

2. **Authority-initiated reporting**, where cyber incident information is gathered by one or more authorities to better understand the effects of its sector-wide implications (and may be performed within or across jurisdictions).

3. **Periodic reporting** of incident-related information gathered from FIs on a regular basis (not event driven), capturing incident occurrences that would not otherwise be reported by FIs through Type 1.

Illustration of reporting types **Figure 6**



Almost all authorities (96%) receive institution-initiated reports, whereas most authorities (78%) also performed authority-initiated or periodic reporting. One authority also responded with an additional type of reporting related to threat reporting, which although valid, was considered outside of the incident reporting scope of the survey.

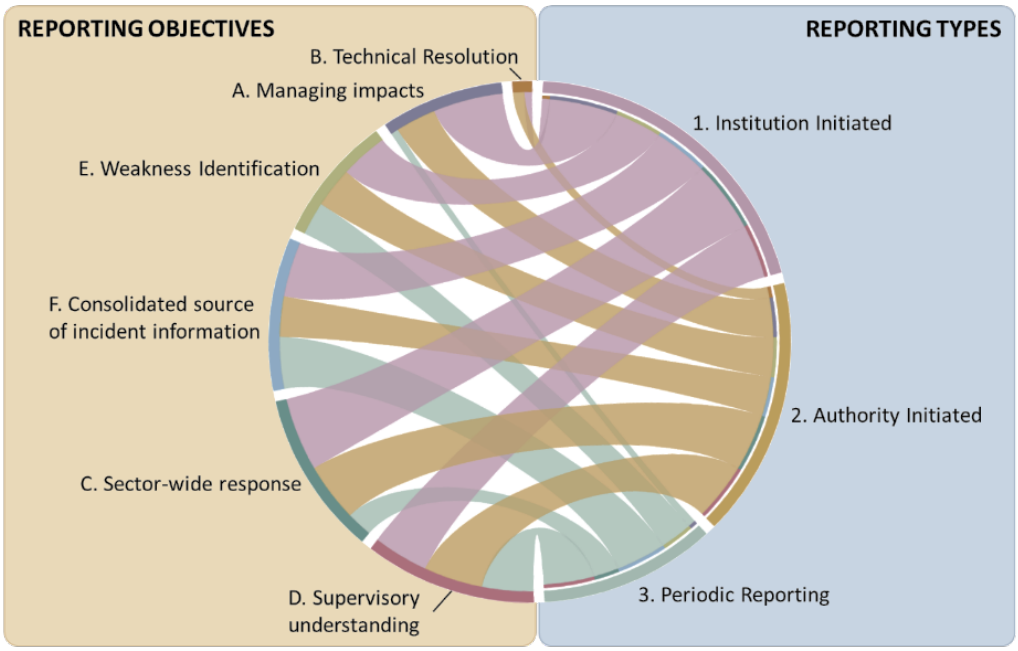
Further analysis of the relationship between reporting objectives and types was performed, (as shown in Graph 4), and the following observations noted:

- There is a strong relationship between event-driven incident reporting (Types 1 & 2) and managing the impacts, either on a firm specific (A) or sector wide basis (C).

- There is a significant relationship between event-driven incident reporting (Types 1 & 2) and developing understanding of institutional capabilities (D), the threats and risks they face, and sectoral trends (F). Periodic reporting (Type 3) is primarily used to reinforce/supplement this understanding.

- Only 63% of respondents use incident information as part of their own regulatory improvement lifecycle (E).

Mapping of Financial Authorities' Reporting Objectives and Reporting Types **Graph 4**



Source: FSB

3. Reporting criteria

For each of the reporting types in Section 2 above which a financial authority chooses to implement, financial authorities will have established mechanisms to trigger each report type, typically reflecting their respective mandates and regulatory or supervisory approaches. Unlike other aspects of CIR where greater convergence is sought, reporting criteria will typically be unique to each authority. However, it may be possible to drive consensus of approach for setting reporting criteria, whilst preserving the act of calibration as an authority-specific activity.

The following analysis sets out the three different ways in which reporting criteria can be designed, such that individual authorities can leverage this information when developing or adjusting their own approaches: (i) overall approach; (ii) reporting trigger selection; and (iii) reporting window design.

Approaches to Reporting Criteria

Based on FSB member survey responses, existing approaches to reporting criteria can broadly be classified on relative basis using two observable measures:

- The degree of detail used to describe the reporting criteria, which can range from minimal, with little to no explanatory guidance, to detailed, with extensive descriptions, indicators and/or examples.

- The criteria style, ranging from purely qualitative expressions of criteria at one end of the spectrum, to quantitative approaches (e.g. numeric thresholds).

Graph 5 represents a comparative, albeit subjective, interpretation of existing authority reporting criteria where provided through the FSB survey. Positioning on the vertical axis (level of detail) was determined based on overall criteria length, number of criteria clauses or examples provided. Positioning on the horizontal axis was assessed on the nature of each individual criteria being assessed as qualitative or quantitative in nature, whereby the mid-point reflects an even mix of both criteria types. Box 2 contains examples reflecting both of these styles.

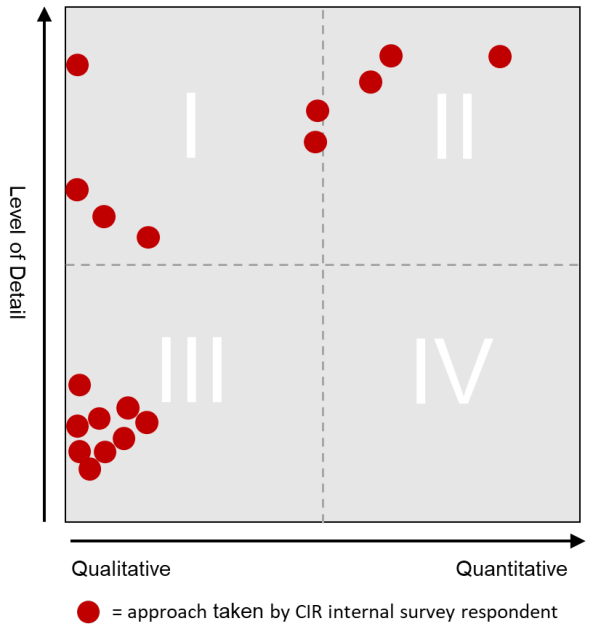
The following observations can be derived from the patterns which emerge:

- There is a notable cluster of authorities that take a 'minimal qualitative' approach, i.e. Quadrant III. For example, an authority may state that regulated FIs should report cyber incidents that generate material levels of impact, but leave institutions to judge when this criteria has been met. Such 'minimal' approaches may incur greater levels of interpretation risk.

- No authorities were observed as using a 'quantitative' but 'minimal' approach (Quadrant IV). This outcome is expected as such approaches typically are accompanied by explanatory information to clarify why such measures have been set.

- Roughly half of authorities that responded have been categorised in the 'detailed' upper half of the graph, though a mix of styles is present, in keeping with authority approaches to policy and rulemaking.

Stylistic comparison of reporting criteria approaches **Graph 5**



Reporting trigger selection

For each reporting type, financial authorities may select from a range of different trigger options which affect the timing and/or timeframe for reporting:

- **Institution-initiated reporting**: the remainder of this section will predominantly focus on this reporting type and the trigger options which exist for initial, intermediate and final reports.

- **Authority-initiated reporting**: the collection of impact assessment information can vary depending on the circumstances, and therefore may be individually determined with each occurrence. Certain cross-authority reporting mechanism may establish pre-agreed norms for timeframes such as the collation and compilation of impact information can be orchestrated.

- **Periodic reporting**: a key consideration for bulk data retrieval from FIs is proportionality i.e. the volume of information collected relative to the frequency of reporting, which may vary in accordance with an institution's systemic importance.

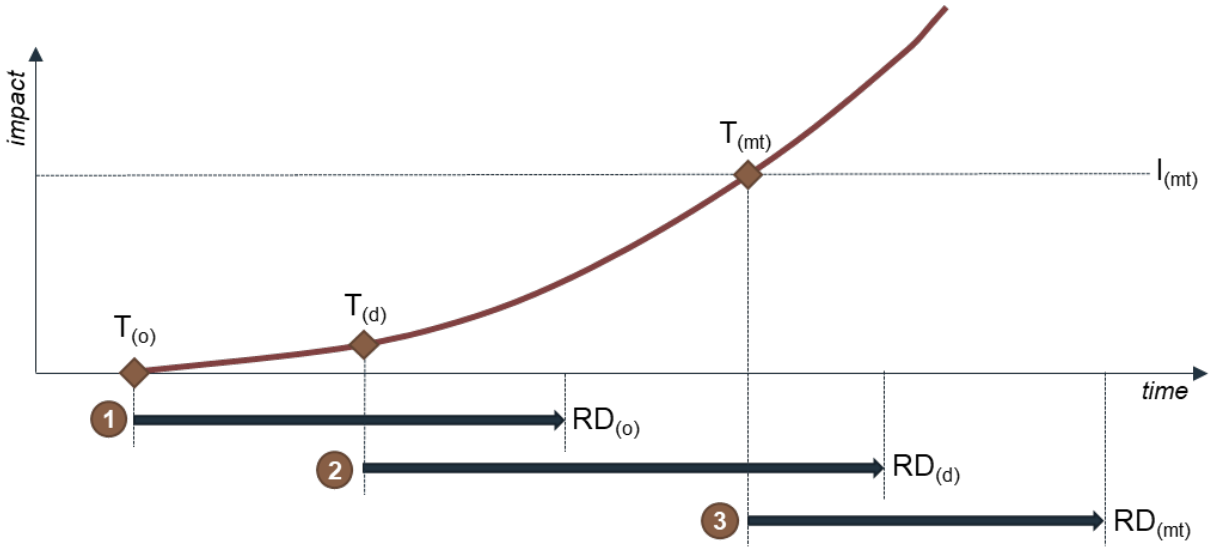
Returning to institution-initiated reporting, and specifically initial reporting, existing financial authority triggers (see Annex C) can broadly be categorised into three types, which are also illustrated in Graph 6:

1. **Occurrence trigger**, based on the time the incident occurred or $T_{(o)}$. With this trigger type, the timeframe by which a FI has to product an initial report by is already passing, even before the incident may have been detected. If the reporting deadline $RD_{(o)}$ passes before detection has occurred, reporting may eventually take place but would by default deemed as a late submission. However, this trigger type may incentivise firms to invest in their detection capabilities such as to minimise the gap between occurrence and detection.

2. **Detection trigger**, based on the time the incident was detected or $T_{(d)}$; As the trigger for reporting only commences when the affected institution becomes aware of the incident, the limiting factor for detection-based reporting is the extent to which the incident circumstances are understood. Where situational confidence is low, it may only be possible to provide limited information before the reporting deadline $RD_{(d)}$ is due.

3. **Threshold trigger**, based on a breach of a materiality threshold or $I_{(mt)}$. Within this option, FIs will judge whether the impacts associated with the incident have breached the materiality threshold, and trigger the reporting obligation $T_{(mt)}$. Although this trigger type can flex to accommodate 'slow-burn' incidents, these triggers rely on a consistent interpretation of reporting criteria, whereas occurrence and detection triggers may be simpler to determine.

Variations in initial reporting triggers **Graph 6**



Legend: $T_{(o)}$ = time of incident occurrence; $T_{(d)}$ = time of incident detection; $T_{(mt)}$ = time at which impacts arising from incident reach/exceed materiality threshold; $RD_{(o)}$ = reporting deadline since incident occurrence; $RD_{(d)}$ = reporting deadline since incident detection; $RD_{(mt)}$ reporting deadline since breach of materiality threshold; $I_{(mt)}$ = level of impact expressed as materiality threshold.

Source: FSB

There are also two further variants of trigger types which authorities could implement:

- **Occurrence or detection triggers, with materiality filters**: To limit the volume of cyber incidents within scope, authorities may apply a materiality filter such that only significant incidents are reported. However, this trigger variant would be based on T(o) or T(d), not T(mt). Because the occurrence or detection trigger has primacy, it may be a source of late reporting, over- or under-reporting for FIs if they cannot reliably estimate if the materiality threshold was crossed by the time the reporting deadline expired.

- **Materiality thresholds with 'likely to breach' clauses**: If reporting is left until a materiality threshold is deemed to have been breached, then the authority only becomes aware of the situation once it has passed this level of impact. This can be offset by requesting that incidents that 'are likely to' breach thresholds are also reported. However, FIs consequently have to also consider the impact trajectory of incidents as part of meeting their reporting obligations.

Whereas the calibration of initial reporting triggers is typically unique to each authority, the equivalent triggers for intermediate and final reports may not have the same drivers:

- **Intermediate report***:* the issuance of additional incident report(s) by the affected institution until the incident is brought under control (i.e. resolved). Analysis of existing reporting templates identified three types of intermediate reporting triggers:

  - *fixed period*, where an intermediate report is expected to be provided on a pre-set schedule e.g. every 24 hours.

- *upon change*, where the affected institution issues a new intermediate report based on a change in circumstances, impact or remediation that an authority might expect to be informed.

- *once resolved*, where an authority does not require updates whilst an incident is still in progress but chooses to be informed once the incident is resolved.

- **Final report***:* the last incident report to be issued following incident closure, and contains the output of any post-incident review (e.g. cause analysis, planned remedial activities). Existing approaches to final report triggers include:

  - *fixed period,* where a final report is expected within a specified time period following incident resolution (e.g. 30 days). As the post-incident review process for significant incidents may be more protracted, additional clauses may be included to allow deviation from the standard period subject to agreement from relevant authorities.

  - *upon closure,* where the final report is issued once the post-incident review has concluded, with no time constraint.

Unlike initial reporting, there may be greater scope for convergence amongst authorities for convergence of these triggers which would support concurrent issuance of intermediate and/or final reports to multiple authorities.

Reporting window design

Having established the criteria that triggers the requirement for a report to be issued, financial authorities are also able to set a timeframe, or reporting window, within which this action needs to be performed. Three characteristics of reporting windows have been identified that authorities can adjust to fit their needs: (i) window type; (ii) language choice; and (iii) duration.

Survey analysis has identified three types of reporting windows:

- **start-bound***,* where the reporting window is anchored at the outset, e.g. ‘immediately’ or ‘as soon as possible’;

- **defined window***,* where both the start and end points of the reporting window are set, e.g. ‘without delay, but no later than 24 hours’

- **end-bound***,* where only the end time of the window is defined, e.g. ‘within 6 hours’

When reviewing each option, authorities may consider the behavioural implications and how FIs may react. For example, an institution may delay the submission of a report which is start-bound to better evaluate the nature or effects of an incident before reporting. Conversely, where a specific end time has been set, FIs may naturally gravitate towards this point, thereby leading the bulk of reports to be received at the tail end of expectations.

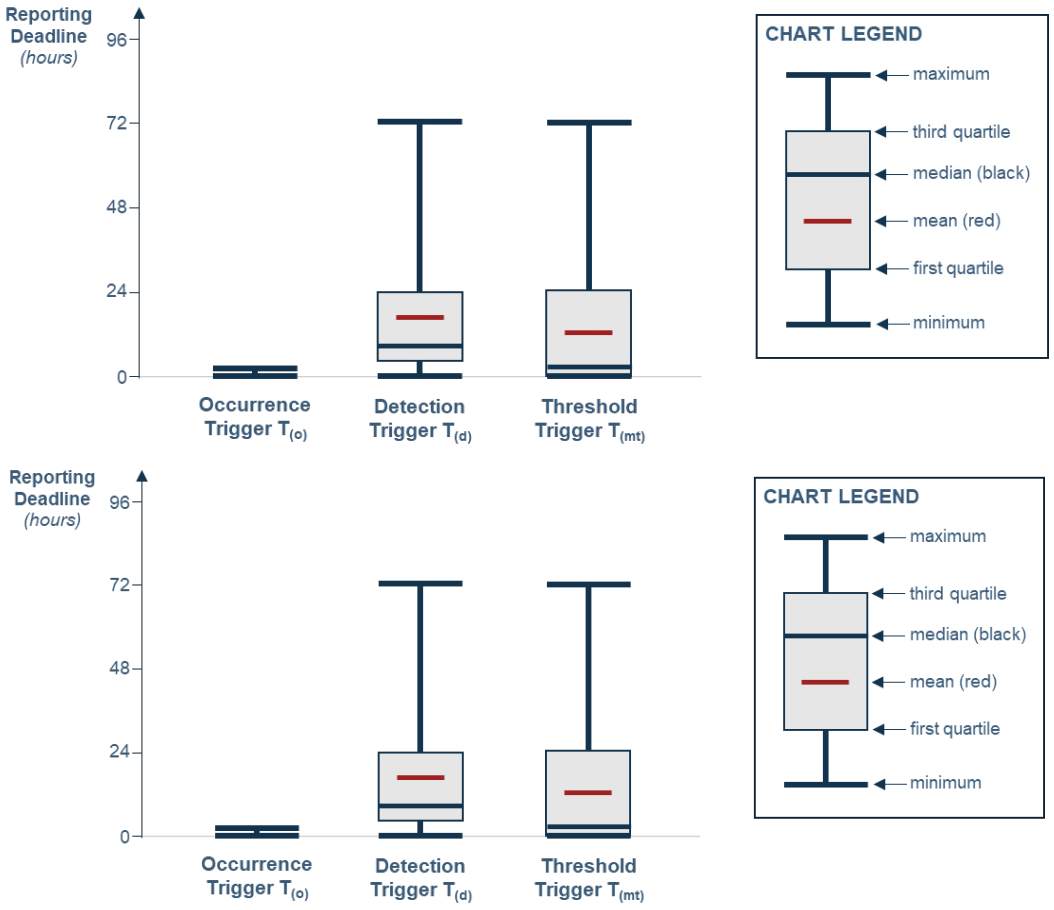
Language choice is a stylistic matter for authorities to consider when drafting reporting window requirements but may be used stress urgency or emphasise a preferred outcome. For example, the use of ‘immediately’ may convey a preference for reporting timeliness, over precision or

completeness. The inclusion of flexible clauses (e.g. as soon as reasonably possible, without undue delay) provides some discretion to institutions when exercising their judgement over how best to satisfy reporting obligations.

On window duration, Graph 7 illustrates the timeframes for initial reporting sourced from references in Annex C, leading to the following observations:

- Very few authorities surveyed implement occurrence triggers, with the remainder being evenly split between detection and materiality-based triggers.
- Although there is a notable spread of window durations for detection and materiality-based triggers (ranging from immediate to 72 hours), the majority fall within a 24-hour timeframe.
- Reporting windows for materiality-based thresholds are slightly tighter than those implemented for detection triggers. A possible explanation for this difference may be that: (i) reporting thresholds for detection-based triggers are more elongated to factor in sufficient time to assess nature of the incident to a reasonable extent; and (ii) if a FI has already determined that a materiality threshold has been reached, then authorities may wish to be rapidly informed that this has occurred.

Box plots of reporting triggers **Graph 7**



Annex B: Recommendations mapped to identified issues and challenges

		Identified issues and challenges					
		Operational challenges	Setting reporting criteria	Culture of timely reporting	Early assessment challenges	Secure communications	Cross-border and cross-sectoral issues
Design of CIR Approach							
1	Establish and maintain objectives for CIR						
2	Explore greater convergence of CIR frameworks						
3	Adopt common data requirements and reporting formats						
4	Implement phased and incremental reporting requirements						
5	Select appropriate incident reporting triggers						
6	Calibrate initial reporting windows						
7	Provide sufficient details to minimise interpretation risk						
8	Promote timely reporting under materiality-based triggers						
Supervisory activities and collaboration between authorities							
9	Review the effectiveness of CIR and CIRR processes						
10	Conduct ad-hoc data collection						
11	Address impediments to cross-border information sharing						
Industry engagement							
12	Foster mutual understanding of benefits of reporting						
13	Provide guidance on effective CIR communication						
Capability Development (individual and shared)							
14	Maintain response capabilities which support CIR						
15	Pool knowledge to identify related cyber events and cyber incidents						
16	Protect sensitive information						

Legend - *degree to which each recommendation, if implemented, address challenges(s)*

None | Minor | Moderate | Significant | Profound

Annex C: Initial reporting trigger reference material

Survey conducted in January 2022

Jurisdiction	Authority	Trigger	RD (hrs)	Source
Australia	**APRA**	Threshold	72 hrs	An APRA-regulated entity must notify APRA as soon as possible and, in any case, no later than **72 hours, after becoming aware** of an information security incident that: (a) materially affected, or had the potential to materially affect, financially or non-financially, the entity or the interests of depositors, policyholders, beneficiaries or other customers; or (b) has been notified to other regulators, either in Australia or other jurisdictions. Source: CPS 234
China	**CBIRC**	Occurrence	Immediate	When cyber security incidents **occur**, network operators should **immediately** initiate an emergency response plan, adopt corresponding remedial measures, and **report to the relevant competent departments** in accordance with relevant provisions. Source: CAC Cybersecurity Law, article 25 (translated) Where the breach, tampering, or loss of personal information **occurs or may occur**, a personal information processor shall **immediately** take remedial measures and **notify the departments** with personal information protection duties and the relevant individuals. *Source: Personal Information Protection Law (PIPL)*
EU	**ECB**	Threshold	2 hrs (SIs)	Initial information on the cyber incident must be submitted within two hours after the reporting thresholds are exceeded or within two hours after the point in time when the Supervised Entity can reasonably assume that an identified cyber incident will exceed the reporting thresholds, whichever occurs earlier. *Source: ECB Decisions (issued directly to the banks in scope)*
	EIOPA	None	N/A	EIOPA does not have incident reporting in place

Jurisdiction	Authority	Trigger	RD (hrs)	Source
	ESMA	Detection	24 hrs	Item 55 / Guideline 62: TRs should send to ESMA an initial incident notification **within 24 hours of becoming aware** of the incident and a follow-up notification within one month. *Source: Guidelines on periodic information and notification of material changes to be submitted to ESMA by Trade Repositories*
	EBA	Threshold	4 hrs	Payment service providers should send the initial report to the competent authority within **four hours** from the moment the operational or security incident has been classified as **major**. *Source: Revised guidelines on major incident reporting under PSD*
France	**BdF**	Threshold Detection Detection	2 hrs (SIs) 4 hrs (retail PSs) 72 hrs (wholesale PSs)	Payment service providers should send the initial report to the competent authority within **4 hours** from the moment the major operational or security incident was first **detected**, or, if the reporting channels of the competent authority are known not to be available or operational at that time, as soon as they become available/operational again. Should business be back to normal before 4 hours have passed since the incident was detected, payment service providers should aim to submit both the initial and the last intermediate report simultaneously (i.e. filling out sections A and B of the template) by the 4-hour deadline. *Source: PSDII (for retail payment systems)* Incident reporting shall occur without any delay **after incident detection** and in less than **72 hours**. *Source: ECB framework for wholesale payment systems (for wholesale payments)*
Hong Kong	**HKMA**	Detection	Same-day	As the nature of every operational incident is different, authorized institutions (AIs) are expected to exercise their judgement and establish internal guidelines endorsed by the management for deciding whether an operational incident should be regarded as significant and thus should be reported to the HKMA. The HKMA expects AIs to report to it suspected or confirmed cyber attacks that

Jurisdiction	Authority	Trigger	RD (hrs)	Source
				may cause potential loss/leakage of sensitive data of the AI or its customer(s), potential financial loss (albeit small) to the affected customer(s), potential material financial loss to the AI, or significant impact on the AI's reputation. The Retail Payment Oversight Division of the HKMA asks SVF licensees to report suspected or confirmed cyber attacks **as soon as practicable**, and to provide prompt updates as and when the information and assessment is available. As for designated CSSs, as long as the incident affects the operation or service level of the system or the safety and efficiency of the system, they should be reported to the HKMA **as soon as possible**. No matter whether the incident is known or unknown to the CSS participant, or whether the incident is caused by a third party or the CSS participant, it should be reported to the HKMA
India	**RBI**	Detection	6 hrs	Guidelines clearly specify reporting requirements for unusual incidents specifying types of incidents to be reported/not reported. At the same time, they also allow for some discretion where FIs can exercise own judgement for reporting the incidents Security Incident Reporting (SIR) to RBI (**within two to 6 hours**) *Source: RBI/2015-16/418*
Indonesia	**BI**	Occurrence	1 hr (PSs)	BI has set qualitative criteria as a reference for CIR; however, no explicit quantitative criteria/ thresholds have been set by the authority. The qualitative criteria includes: potential breaches to the legal/regulatory requirements and the materiality of impact to the critical information systems or services which could cover malfunctioning data centres, network failures, and fraud incidents. Article 254.6: The disruption as referred to in paragraph (5) point c and force majeure as referred to in paragraph (5) point d must be notified to Bank Indonesia **not later than 1 (one) hour after the disruption occurrence**.

Jurisdiction	Authority	Trigger	RD (hrs)	Source
				Source: Bank Indonesia Regulation Number 23/6/PBI/2021 (Payment Service Providers)
Italy	**BdI**	Threshold Threshold Detection	2 hrs (SIs) 4 hrs (LSIs) 3 hrs (PSs)	Regarding the timing of notification of incidents, the initial report must be sent: • for less significant banks, payment and electronic money institutions within **4 hours** from the moment when the reporting criteria are met • for significant banks within **2 hours** from the moment when the reporting criteria are met • for retail payment systems, payment schemes and financial technology providers within **3 hours of incident detection**
	MEF	Threshold	1-6 hrs (OES/ DSPs)	As for the national security cyber regulation n. 81/2021 for the financial operators included in the National Cybernetic Perimeter (Law n. 109/2019), the notification mechanism is threshold-less and based on the definitions of relevant cyber events. Designated critical national infrastructure must notify CSIRT Italy without delay of any incident having a significant impact on the continuity of the essential services provided, including information that makes it possible to identify cross-border impact of the incident. The notification must be made **within six hours or one hour** depending on the severity of the incident. *Source: Italian Legislative Decree no. 85/2018*
Japan	**JFSA**	Detection	Immediate	The FSA requires FIs to report **immediately** when a computer system failure or a cyber security incident meeting certain criteria is **detected**. Criteria for reportable incidents are provided in FSA's supervisory guidelines. Similar provisions are in place in FSA's supervisory guidelines for other types of FIs. Form 4-45 'Report of System Failure and Other Incidents' in the 'Forms and Other Materials' shall be submitted as part of the reporting. Additional reporting is required upon recovery and/or when cause of the incident is identified. A status update shall

Jurisdiction	Authority	Trigger	RD (hrs)	Source
				be reported within one month if the recovery or identification of the cause has not been completed. *Source: Comprehensive Guidelines for Supervision of Major Banks, III-3-7-1-3: Supervisory methods and actions*
Russia	**CBR**	Detection Detection	3 hrs (SIs) 24 hrs (Other)	Significant Institutions: within **three hours** from the moment of **detection** of the incident. Other institutions: within **24 hours** from the moment of **detection** of the incident *Source: Bank of Russia Standard STO BR BFBO-1.5-2018 (Section 6)*
Saudi Arabia	**SAMA**	Threshold	Immediate	The Member Organisation should inform 'SAMA IT Risk Supervision' **immediately** when a medium or high classified security incident has **occurred and identified**. *Source: Cyber Security Framework v1.0, Article 3.3.15.5*
Singapore	**MAS**	Detection+ Threshold	1 hr	A bank shall notify the Authority **as soon as possible, but not later than 1 hour**, **upon the discovery** of a relevant incident. • 'relevant incident' means a system malfunction or IT security incident, which has a severe and widespread impact on the bank's operations or materially impacts the bank's service to its customers. *Source: MAS Notice on Technology Risk Management*
Spain	**BdE**	Threshold	2 hrs	**Two hours from its qualification** as relevant *Source: LSI reporting template (ECB Framework)*
Switzerland	**FINMA**	Detection	24 hrs	If a cyber attack on critical assets results in one or more of the protective goals of critical functions and their business processes being put at risk, this must be reported to FINMA immediately. Immediate reporting to FINMA means that the affected supervised institution informs FINMA through the responsible (Key) Account Manager **within 24 hours of detecting such a cyber attack** and conducting an initial assessment of its criticality. The actual report should be **submitted within 72 hours** via the FINMA

Jurisdiction	Authority	Trigger	RD (hrs)	Source
				web-based survey and application platform (EHP). *Source: FINMA*
Türkiye	**BRSA**	Occurrence	N/A	A firm must notify the BRSA **immediately** if any sensitive or personal data are disclosed or leaked such that Information Systems Continuity Plan or secondary centres are activated. *Source: Regulation on Information Systems and Electronic Banking Services of Banks*
UK	**BoE (PRA)**	Threshold	Immediate	A firm must notify the PRA **immediately if it becomes aware**, or has information which reasonably suggests, that any of the following has occurred, may have occurred or may occur in the foreseeable future: (1) the firm failing to satisfy one or more of the threshold conditions; or (2) any matter which could have a significant adverse impact on the firm's reputation; or (3) any matter which could affect the firm's ability to continue to provide adequate services to its customers and which could result in serious detriment to a customer of the firm; or (4) any matter in respect of the firm which could result in serious financial consequences to the UK financial system or to other firms. *Source: PRA Rulebook, 2.1 General Notification Requirements*
	FCA	Threshold	Immediate	A firm must notify the FCA **immediately if it becomes aware**, or has information which reasonably suggests, that any of the following has occurred, may have occurred or may occur in the foreseeable future: (1) the firm failing to satisfy one or more of the threshold conditions; or (2) any matter which could have a significant adverse impact on the firm's reputation; or (3) any matter which could affect the firm's ability to continue to provide adequate services to its customers and which could result in serious detriment to a customer of the firm; or

Jurisdiction	Authority	Trigger	RD (hrs)	Source
				(4) any matter in respect of the firm which could result in serious financial consequences to the UK financial system or to other firms. *Source: FCA Rulebook, SUP 15.3 General Notification Requirements*
US	**FRB**	Threshold	36 hrs (Banks)	The Federal Reserve Board, OCC, and FDIC issued a final rule that requires a banking organisation to notify its primary federal regulator of any 'computer-security incident' that rises to the level of a 'notification incident,' as soon as possible and no later than **36 hours** after the banking organisation determines that a **notification incident has occurred**. A bank service provider is required to notify at least one bank-designated point of contact at each affected customer bank as soon as possible when it determines it has experienced a computer-security incident that has materially disrupted or degraded, or is reasonably likely to disrupt or degrade, covered services provided to the bank for four or more hours. *Source: Computer-Security Incident Notification Requirements for Banking Organisations and Their Bank Service Providers*
	SEC Rule (SCI Entities)	Threshold	Immediate	SCI personnel having a reasonable basis to conclude that an SCI event has occurred must notify the Commission. *Source: SEC Regulation SCI (17 C.F.R. §§ 242-1002)*