Challenges to achieving greater convergence in CIR (Section 2)

1. Is the emphasis on practical issues to collecting and using cyber incident information consistent with your experience? Does your institution want to provide any additional evidence for the FSB to consider from your experience?

Yes, the emphasis on practical issues to collecting and using cyber incident information is consistent with our experience.

Concerning the "*Cross-border and cross-sectoral issues*", Intesa Sanpaolo considers that beyond the financial sector, the need for incident reporting harmonization in a cross-industries & cross-borders perspective is a strong and pressing issue. We **note a lack of common criteria in the various regulations and thresholds for reporting incidents**. In fact, as reported by the paper, the calibration of reporting criteria is often specific to each financial authority, but **there is a need of common criteria and thresholds involving different incident reporting regulations**.
When looking at **cross-borders interaction the approach is twofold**. In a **bottom-up perspective**, each private entity has to assess which are the local jurisdictions applicable to its geographic presence. From a **top-down perspective**, in most cases legislators have identified a need for cross-border cooperation. However, this relies upon the communication among National Competent Authorities, and generally the legislations foresee a central entity at EU level that shall be informed by the National Competent Authority.

Intesa Sanpaolo highlights two aspects that should be considered regarding the Incident Reporting workflows to make them more effective, and to move towards a more proactive incident reporting framework, namely:

- It shall be appropriate to reconsider the workflow to introduce a **bi-directional information flow**.
- It is unclear how the different Supervisory Authorities do communicate with each other to be able to leverage to the greatest extent the sharing of relevant information.

Banks are **often subject to multiple regulations and consequently to multiple reporting requirements** for one incident with consequent fragmentation, multiple reporting, different thresholds, excessive effort for reporting to the various authorities involved.
The latest regulatory developments have introduced new requirements in data security, info-sharing, incident reporting and crisis management. The frameworks for Incident reporting, arising from these developments, imply the involvement of multiple authorities at National, European, and international level, applying different procedures and templates, creating possible overlaps and redundancy in the process of information reporting.
We hope that the introduction of the DORA-Digital Operational Resilience Act will facilitate reporting obligations since one of its goals is to facilitate and harmonize incident reporting and the incident management landscape.
As regard the practical issues "*Culture of timely reporting*" and "*Early assessment challenges*", Intesa Sanpaolo believes that the **mandatory incident reporting frameworks indeed require very often a very tight timeline for the incident notifications.** This means that the Incident Management Team must take care of the incident management reporting in parallel with the incident management and the recovery procedure.

Recommendations (Section 3)

2. Can you provide examples of how some of the practical issues with collecting and using cyber incident information have been addressed at your institution?

We want to underline some main challenges that we see in our experience:
First, there is a lack of harmonization. In particular:

- Financial institutions are **subject to multiple regulations and to multiple reporting requirements** for one incident with consequent fragmentation, multiple reporting, different thresholds, excessive effort for reporting to the various authorities involved.
- The latest regulatory evolutions have introduced new requirements in data security, info-sharing, incident reporting and crisis management. These new frameworks for Incident

reporting, imply the involvement of multiple authorities at National, European, and international level, requiring different procedures and templates, creating possible overlaps and redundancy in the process of information reporting.

- We hope that the introduction of the DORA at European level will facilitate reporting obligations since one of its goals is to facilitate and harmonize incident reporting and the incident management landscape.
- Even though harmonization of incident reporting obligations is a well-known issue, we acknowledge that new requirements will be introduced. The latest two are: the Cyber Resilience Act (CRA) and U.S. Cybersecurity and Infrastructure Security Agency (CISA) request for information (RFI) on reporting requirements for cyber incident reporting.

In addition, we must provide different information for different jurisdictions:

- Being a multinational company, we also need to comply with different regulations. While we **try to have a comprehensive view of threat landscape, we struggle to have** a common understanding of information about cyber incidents that can be helpful

3. Are there other recommendations that could help promote greater convergence in CIR?

To promote a greater convergence in CIR, Intesa Sanpaolo suggests leveraging the idea of **a centralised Hub**, which will be subject to a feasibility study by the European Supervisory Authorities according with the DORA, and which would receive all mandatory incident reporting. The EU Hub structure and "format" can be **leveraged by other jurisdictions** to create similar hubs and have a **network at global level** to deal with cyber crises.

We suggest a **two-step path for the adoption of the Central Cyber Incident Reporting Hub** at European level, for the new structure to evolve gradually and to reach a final high level of efficiency. As a **first step**, we suggest that reports continue to be sent to the competent authorities, while **periodically** (for example, monthly) such reports are **also to be sent to the Hub** for information. In this phase, we envisage to start the adoption of a **common template** for mandatory incident reporting. This phase will help the Hub to collect information about existing mandatory incident reporting requirements among the Member States. As a **second step**, we suggest that **the Hub directly receive the mandatory incident notifications and related reports by the Financial Institutions**, and then **dispatches them to the different competent authorities, in line with specific communications' timelines**. In this phase, we will see the importance of the previous adoption of a single template, replacing the several reports already in force. In this context, the definition of a **standard that provides for a single taxonomy and a single method of classification** of incidents is even more important to make the information transmitted immediately comparable and to improve cooperation at EU level. In the second step, the Hub will learn about the different member States' competent authorities thanks to the first step, when it received all the reports prepared by the Financial Institutions.

There is also a need for a **common taxonomy** to then better detail it, but also for the **classification methodology**.

We understand the difficulty considering that the methodology shall apply to different regulatory requirements, and it is difficult to make a neutral version of it, but we believe it is possible to achieve a standard methodology using common principles (e.g., impacted customer / total customer ratio).

In addition, crisis management and the response part of Cyber Incident Management process should be streamlined and integrated. A **clear set of harmonized rules** would be beneficial to comply properly and smoothly to the mandatory incident reporting requirements; a sound incident reporting model improves the clarity of what happens, an adequate sharing of information and a trusted cooperation with all stakeholders.

4. Could the recommendations be revised to more effectively address the identified challenges to achieving greater convergence in CIR?

With the review of the NIS Directive and the new Digital Operational Resilience Act (the DORA), we see the first steps towards the harmonization of incident reporting requirements, at least for the financial sector. The **focus should be on a common taxonomy, voluntary information sharing, further incident reporting harmonization, and possibly, the creation of a centralized EU Incident HUB, as mentioned in the DORA proposal**.

The aims should be to join the efforts in **identifying the best possible options** not only to address the compliance to the existing incident reporting requirements, but also to dialogue with the EU institutions and legislators to **create synergies, improvements, increasing efficiency, decreasing costs,** and reducing the effort and the time needed to complete (perform?) the obligatory incident reporting-related activities. To increase the efficiency of coordination between organizations and to reduce incident reporting burden, it is necessary to streamline and enhance current reporting initiatives through a common and standardized taxonomy, managed from a central and shared point. One possible solution is the **establishment of a centralised Hub (as reported in DORA Regulation)**, at European level, which would receive all mandatory incident reporting.

Regarding the eight recommendations, "*Extend materiality-based triggers to include likely breaches*" Intesa Sanpaolo doesn't fully agree with it and supports instead clear and well-defined thresholds for the incident notification, and it is against to the mandatory reporting of any likely threat. This would entail additional burdens for the financial entity and, furthermore, the risk of creating an over-reporting landscape.

Common terminologies for CIR (Section 4)

5. Will the proposed revisions to the Cyber Lexicon help to encourage greater adoption of the Cyber Lexicon and promote greater convergence in CIR? Are there any other ways in which work related to CIR could help to encourage greater adoption of the Cyber Lexicon and promote greater convergence in CIR?

Intesa Sanpaolo believes that there is a strong need to have **a common understanding of terms and standards on cyber incidents**. In order to avoid a new regulatory burden on financial entities, we recommend that definitions are **aligned with those already adopted at international level** and to avoid overlapping/duplication with already existing legislations on ICT risk management or with rules that are to be adopted.

Furthermore, it is necessary **to create a common taxonomy and common classification criteria**. We believe that if quantitative and well-defined parameters for incident classification are not considered, it is impossible to reach convergence in incident reporting. I**t is necessary to establish clear common thresholds and define a clear methodology to classify incidents.**

6. Do you agree with the definition of 'cyber incident,' which broadly includes all adverse events, whether malicious, negligent or accidental?

Intesa Sanpaolo recommends that definitions are aligned with those already adopted at international level.
We agree to include in the 'cyber incident' definition all adverse events, whether malicious, negligent, or accidental, since a cyber incident could be caused both by a cybercriminal and by accidental actions.

7. Are there other terms that should be included in the Cyber Lexicon to cover CIR activities?

We proposed to add to the cyber lexicon also **a common taxonomy to classify incidents**.
In addition, we noted that from the analysis of the Cyber Lexicon, the term related to **Cyber Impact Assessment** is absent. It could be useful to add it to have a common understanding of impact matrices.

8. Are there other definitions that need to be clarified to support CIR?

We proposed to define **a common methodology to classify incidents** to have clear parameters in case of incident to classify it and to perform correct notifications to the authorities.
From the analysis of the Cyber Lexicon, the term "*Data Breach*" does not refer specifically in the case of compromise of personal/sensitive data.

Format for Incident Reporting Exchange (FIRE) (Section 5)

9. Would the FIRE concept, if developed and sufficiently adapted, usefully contribute towards greater

convergence in incident reporting?

Yes, FIRE concept **could be useful since it establishes a common template** to be filled in, in case of incident and it contributes to reach greater convergence in incident reporting. Anyway**, we notice a lack of common thresholds**.

Although FIRE concept is already a step forward and it could be very useful to have a common template, we note a lack of common thresholds for carrying out incident reporting and of a standard methodology that allows financial institutions to understand when or not to carry out incident reporting.

In addition, FIRE template should be used for all regulations that require incident notification, to have a common template filled in, in case of incident.

10. Is FIRE readily understood? If not, what additional information would be helpful?

We point out that the **"lessons" section** in some case could be filled in after a long time after the incident has occurred, as in most case it takes time to investigate the incident roots and causes and to find corrective actions that prevent the incident from occurring in the future.

Furthermore, in addition to the FIRE template, **a single-entry point** could be useful to report incidents to it. A single incident might entail the need to report to different Authorities and a great burden for a financial entity to satisfy all requests and clarifications from the authorities. Therefore, we suggest combining FIRE with a single-entry point on a European basis for reporting incidents, which will then notify the incident to the individual authorities and stakeholders involved.

In addition, it could be useful to add in the FIRE template **a specific field with the regulation** that requires the reporting activity.

11. If FIRE is pursued, what types of organisations (other than FIs) do you think would need to be involved?

Beyond the financial sector, the need for incident reporting harmonisation in a **cross-industries & cross-borders perspective** is a strong and pressing issue. Reducing differences with non-banking industries would increase the level playing field and enhance the whole European ecosystem resilience, considering the interrelationships and interconnections between different industries. Therefore, we suggest applying FIRE to all entities, not only financial ones and to implement **an EU centralised Incident Hub. This will lead** to **create synergies, improvements, increasing efficiency, decreasing costs and a better EU cross sectorial collaboration.**

12. What preconditions would be necessary to commence the development of FIRE?

The preconditions that would be necessary to commence the development of FIRE are the establishment of **impact thresholds for the different incidents** and the definition of a common taxonomy for the incidents classification with relative methodology applied. Furthermore, it is necessary that all regulations concerning incident reporting refer to FIRE, to have a common template.