


POSITION PAPER



WSBI-ESBG response to the Financial Stability Board's consultative document on Cyber Incident Reporting

WSBI (World Savings and Retail Banking Group)
ESBG (European Savings and Retail Banking Group)

Rue Marie-Thérèse, 11 - B-1000 Brussels

ESBG Transparency Register ID 8765978796-80

December 2022



WSBI



ESBG



Introduction

On 17 October 2022, the FSB published a [consultative document](#) on Achieving Greater Convergence in Cyber Incident Reporting. The FSB is inviting feedback on this document.

Back in 2021, the FSB already published a [report](#) on Cyber Incident Reporting: Existing Approaches and Next Steps for Broader Convergence. The report set out three ways the FSB would take work forward to achieve greater convergence in cyber incident reporting (CIR): (i) develop best practices; (ii) create common terminologies for CIR; and (iii) identify common types of information to be shared across jurisdictions and sectors.

To inform its work, the FSB conducted a survey of FSB members to: identify the most common reporting objectives and types of reporting performed; understand the practical issues financial authorities and financial institutions (FIs) have in collecting or using incident information; identify the information items authorities collect to meet the common reporting objectives, including a review of existing incident reporting templates; and explore the mechanisms for financial authorities to share incident information across borders and sectors.

Drawing on the survey findings, the FSB has set out recommendations to address impediments to achieving greater convergence in CIR with a view to promote better practices. This work also helped to inform refinements to the [Cyber Lexicon](#), which resulted in the addition of four terms and revision of three definitions. The FSB also reviewed financial authorities' incident reporting templates and identified commonalities in the information collected. Leveraging on this work, the FSB presents a concept for a format for incident reporting exchange (FIRE) to promote convergence, address operational challenges arising from reporting to multiple authorities and foster better communication.

The FSB is inviting feedback on this [consultative document](#), in particular on the questions set out in the sections below. Responses will be published on the FSB's website unless respondents expressly request otherwise.

1. 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?

Similar reports are requested on the same subject, with a slightly different taxonomy, filtering criteria, or other requirements. This is imposing costs and efforts to the bank without a tangible or visible benefit. Reports on the same subject matter should be better harmonised between different regulatory bodies, processes, and data requests. We encourage regulators to align on a unified cyber/ICT incident data set that allows them to create custom reports without the need for remapping, modification, or ad-hoc reporting on the side of the bank.



2. 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?

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

Financial authorities should offer tools and/or platforms that minimize operational issues for reporting of incidents. For instance, the usage of Spreadsheets using 'ActiveX' does not allow the fill out using Apple OSX workstations or Office 365 web-apps; handling of PGP certificates for encryption of mail-content also quite often comes with operational issues in handling.

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

Please see questions 3.

3. 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?

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

To our understanding, the term 'cyber incident' is unclear or potentially misleading in the sense that it is by definition limited to 'cybersecurity incidents' only. Operational incidents, e.g. due to human error leading to unavailability of a system/service, seem to be excluded from this definition.



Certain reporting obligations are focusing on 'operational or security incidents', which would make it hard to map these reporting obligations if a mixture is used.

We propose to clearly differentiate between the terms 'cyber incident' and the subcategory thereof of 'cybersecurity incident'. The terms should not be mixed, nor should the term 'cyber incident' be used to refer to 'cybersecurity incidents'.

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

Both terms, 'cybersecurity incident' and 'cyber incident', should be added to the lexicon. To our understanding, 'cyber incident' is the top-level category that also includes ICT incidents such as system failures, whereas as 'cybersecurity incident' is a sub-category thereof with malicious human actors as key risk drivers. Next to 'cybersecurity incident' also 'operational incidents/operational cyber incidents' should be considered.

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

It is important to clearly distinguish what is in scope, to ensure a clear understanding of terms like 'cyber event', 'cyber incident', 'cyber security incident' and other ICT incidents to avoid confusion.

4. 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?

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

Is it correctly understood that in "phased reporting" still all group data fields are intended to be reported?

Practically, it has been identified as a benefit to have initial reporting, requiring only to provide a very limited amount of info about the incident, in order to not hinder the operational incident resolution. Information on actors, impact assessments, and root cause analysis should be mandatory for reporting on a later stage.



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

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



About ESBG (European Savings and Retail Banking Group)

ESBG is an association that represents the locally focused European banking sector, helping savings and retail banks in 16 European countries strengthen their unique approach that focuses on providing service to local communities and boosting SMEs. An advocate for a proportionate approach to banking rules, ESBG unites at EU level some 885 banks, which together employ 656,000 people driven to innovate at 48,900 outlets. ESBG members have total assets of €5.3 trillion, provide €1 trillion billion in corporate loans, including SMEs, and serve 163 million Europeans seeking retail banking services. ESBG members commit to further unleash the promise of sustainable, responsible 21st century banking. Learn more at www.wsbi-esbg.org.



European Savings and Retail Banking Group - aisbl
Rue Marie-Thérèse, 11 ■ B-1000 Brussels ■ Tel: +32 2 211 11 11 ■ Fax : +32 2 211 11 99
Info@wsbi-esbg.org ■ www.wsbi-esbg.org

Published by ESBG. [December 2022]