Bundesverband der Deutschen Volksbanken und Raiffeisenbanken e. V.
Bundesverband deutscher Banken e. V.
Bundesverband Öffentlicher Banken Deutschlands e. V.
Deutscher Sparkassen- und Giroverband e. V.
Verband deutscher Pfandbriefbanken e. V.

Die Deutsche Kreditwirtschaft

Achieving Greater Convergence in Cyber Incident Reporting

GBIC Response to the FSB Consultative Document on October 17, 2022

Lobby Register No R001459

Contact:
Diana Campar
Associate Director
Telephone: +49 30 1663-1546
E-Mail: diana.campar@bdb.de

Berlin, 30 December 2022

The **German Banking Industry Committee** is the joint committee operated by the central associations of the German banking industry. These associations are the Bundesverband der Deutschen Volksbanken und Raiffeisenbanken (BVR), for the cooperative banks, the Bundesverband deutscher Banken (BdB), for the private commercial banks, the Bundesverband Öffentlicher Banken Deutschlands (VÖB), for the public banks, the Deutscher Sparkassen- und Giroverband (DSGV), for the savings banks finance group, and the Verband deutscher Pfandbriefbanken (vdp), for the Pfandbrief banks. Collectively, they represent approximately 1,700 banks.

Coordinator:
Bundesverband deutscher Banken e. V.
Burgstraße 28 | 10178 Berlin | Germany
Telephone: +49 30 1663-0
www.die-deutsche-kreditwirtschaft.de
www.german-banking-industry.org

GBIC **Response to the FSB Consultative Document on October 17, 2022**

General comments

In the context of rising cyber incidents[1] and a dynamic cybersecurity threat landscape, it is a very important goal to achieve better convergence in information sharing between financial institutions and authorities in both communication directions.

By eliminating the existing divergence, the protective goals of cybers incident reporting can be better achieved and help institutions bring significant cybersecurity incidents under control and prevent economic damage to their own organizations. Greater convergence will also enable more effective, targeted, and timely communication among relevant authorities to strengthen general financial stability.

As noted in the consultation paper, we believe the new Digital Operational Resilience Act (DORA) is also an important step in harmonizing cybersecurity incident reporting requirements. The aim of harmonization here should be to establish a reporting system that is as uniform and centralized as possible across multiple recipients in the EU, and thus also to improve the cross-border exchange of information and cooperation between the competent authorities in the member states.

The German Banking Industry Committee (GBIC) is pleased to comment on the Financial Stability Board's (FSB) consultation paper "Achieving Greater Convergence in Cyber Incident Reporting". We very much welcome the FSB's efforts to achieve greater harmonization in the reporting of cyber incidents and would like to comment below on selected issues and recommendations of the overall very successful consultation paper.

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?

The challenges outlined by the FSB in the current CIR are largely consistent with the experience of financial institutions. We would like to comment on some of the challenges as follows:

- Operational challenges

The different reporting timeframes, reporting criteria, and reporting formats for different recipients slow down reporting and tie up resources at financial institutions that are needed to remediate the incident. In the sense of DORA, uniform reports should be made to a central reporting point, from where they can be forwarded to other relevant authorities.

The definitions and reporting criteria must be uniform, sufficiently detailed, consistent and practice-oriented. The fixed thresholds for classifying incidents should be designed to be practical. The reporting criteria must be based on the impact on the institution and the extent to which the customer is affected.

[1] e. g. https://www.bka.de/SharedDocs/Downloads/DE/Publikationen/JahresberichteUndLagebilder/Cybercrime/cybercrimeBundeslagebild2021.html (page 5)

The complexity - at least of the initial reports - must be reduced to allow for a fast understanding of the incident and timely reporting.

It must be possible to easily withdraw the initial reporting if it becomes evident further down the line that the reporting thresholds have not been exceeded.

Different authorities should jointly define uniform criteria for both the initial reporting and the subsequent reporting. This would also make it easier for the authorities to communicate with each other.

- Culture of timely reporting

We can only partially confirm the challenges for timely reporting by our experience. The following two points are significant for complicating timely reporting from a practical perspective:

- Depending on the type of incident, early detection and assessment can be difficult on a case-by-case basis.[2]

- The complexity of the reporting requirements further complicates early reporting.

For these reasons, some flexibility should be provided in the initial reporting in order to be able to quickly report the most important information about an incident, combined with the possibility of an uncomplicated withdrawal of the reporting in the case that the incident is classified as not required to be reported in the further stage.

In addition, it should be allowed for IT service providers to report incidents on a consolidated basis on behalf of financial institutions affected by the incident (giving details of the institutions affected). Service providers can describe the incidents and their causes precisely, multiple reporting of the same incident by financial institutions is avoided, and there is no delay in incident reporting that would result from the information chain service provider - financial institution. In Germany, consolidated PSD2 reporting to supervisors is already enabled.

- Secure communications

Multiple reporting channels are operational and security challenges.

- Cross-border and cross-sectoral issues

Data protection and security-related aspects for cross-border information exchange should be regulated uniformly for all the receiving parties.

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?

[2] e. g. https://www.ibm.com/reports/data-breach (page 14, fig. 8)

All activities have been centralized around the response team. Depending on the kind of breach it contacts all necessary stakeholders (e.g., data protection) in order to create and report to regulators if mandatory.

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

Authorities should provide regular feedback on reporting received and be proactive in providing appropriate information in the case of potential risk to other institutions. The feedback should be provided in a way that other financial institutions can derive appropriate insights from it.
Regardless of individual cases, the authorities should provide a summary of events on a regular basis (e.g., semi-annually or annually).

Cooperation between the various authorities should be well coordinated, especially in the case of public communication, to ensure targeted and effective information while avoiding negative effects on companies in the public eyes.

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

- We propose to amend the 1st recommendation as follows:

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

In Europe, a uniform framework can be aligned with the ECB incident reporting form.

- We propose to amend the 3rd recommendation as follows:

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

Platform-independent standard formats should be used for reporting, both in English and the national language.

- Comments on 6th recommendation:

Financial authorities should consider when defining reporting parameter (aka reporting windows) like timeliness, language and frequency how these parameters impact quality and completeness of reporting. This applies for initial reporting and subsequent incident reporting.

In particular, intermediate reporting should be based only on new findings and not on a set timetable.

- Comments on 8th Recommendation:

Likely breaches should not be subject to mandatory reporting, but there should be the possibility of voluntary initial reporting and simple withdrawal of reporting if the thresholds are not exceeded. This recommendation should not lead to unclear definitions of the thresholds.

- Comments on the 13th recommendation:

The recommendation should be considered in the context of a uniform framework and in the context of the recommendation under 12.

- Comments on the 15th recommendation:

The recommendation should be implemented both nationally and internationally.

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?

Generally, the Cyber Lexicon should be aligned with industry standards.

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

Potential incidents and operational and technical issues should not be included in the definition; operational incidents and malicious cyber incidents must in principle be treated differently. The focus of this consultation should be on the reporting of cybersecurity incidents, as these (unlike operational incidents) may pose a potential risk also to other institutions and to general financial stability. Bi-directional information sharing between financial institutions and reporting authorities can flank the defensive measures of the affected institution and other potentially vulnerable organizations. For this reason, it would be useful to include a separate definition for non-motive-based operational incidents.

The proposed definition of "cyber incident" should be revised. The proposed language "violates the security policies, security procedures, or acceptable use policies whether resulting from malicious activity or not" should be removed from the definition. This language is too broad and does not focus on the impact to the firm.

The term "significant impact" should be added, and this definition should be the only trigger for mandatory reporting.

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

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

It is not evident in the consultative document who will be responsible for maintaining the database in which the information submitted using FIRE will be stored. Also, the FSB should explain the measures for

security and retention of the data. This will give participants some level of confidence that the information they provide will be stored securely and will not be at risk of being stolen or otherwise compromised.

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

At the EU level, the development of the FIRE concept should be coordinated with the upcoming second-level regulation on the adopted DORA regulation.