

22 December 2022

Secretariat to the Financial Stability Board  
Bank for International Settlements  
Centralbahnplatz 2  
CH-4002 Basel  
Switzerland  
Via Email: [fsb@fsb.org](mailto:fsb@fsb.org)

Doc Ref: BENJAMINA/#319345\_V1  
Your ref:  
Direct ☎: +27714721250  
E-✉: BenjaminA@banking.org.za

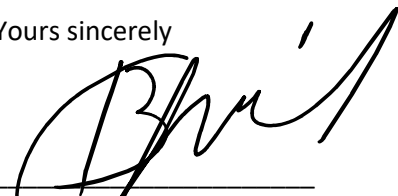
Dear Sir/Madam

**CONSULTATIVE DOCUMENT: CYBER INCIDENT REPORTING CONVERGENCE**

The Banking Association of South Africa (“BASA”) and its members appreciate the opportunity to comment on the Consultative Document: Achieving Greater Convergence in Cyber Incident Reporting, as part of the informal consultation with the industry.

BASA has consulted with its members in respect of the proposed prudential standard and comments are below.

Yours sincerely



---

**B April**  
**General Manager - Prudential Division**

NAME OF PERSON COMPILING SUBMISSION: Benjamin April  
 ORGANISATION: The Banking Association South Africa  
 SUBMISSION DESCRIPTION: FSB Consultative document on Achieving Greater Convergence in Cyber Incident Reporting

NR	REFERENCE IN ACT/BILL/DOCUMENT	COMMENT (Why is it a problem?)	PROPOSED WORDING/COMMENT
1.	Recommendation 2	The scope is “Financial authorities,” and this may need to expand, for example, to cover data protection regulators, given the overlap often found between cyber incidents and data breaches.	<b>Recommend</b> expanding the scope to cover both financial authorities and broader regulatory bodies.
2.	Challenges to achieving greater convergence in CIR (Section 2)	Is the emphasis on practical issues in 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?	<p>The practical issues discussed in the document are consistent with experience.</p> <p>Overall, agree with the challenges referenced, specifically “operational issues” and “inconsistent definitions and taxonomies” are prevalent blockers to consistent reporting.</p> <p><u>Inconsistent Taxonomy:</u> There are inconsistencies in reporting cyber incidents (differences in timing, reporting formats and mechanisms) per regulator.</p> <p><u>Inconsistent Definition:</u> There is also no clarity on the difference or overlap between cyber, information, technology change and privacy incidents.</p> <p><u>Operational Issues:</u> Challenges in collecting all the relevant information and ensuring all the relevant forms (which are all different with different requirements) are completed.</p>
3.	Recommendation 3	Likely to be most effective and successful to adopt a common reporting format by financial authorities within a single jurisdiction as that is the most “pain” is experienced.	<p><b>Recommend</b> the scope be expanded to achieve standardisation across the different regulators within each country.</p> <p><b>Recommend</b> a hybrid approach, where a base set of fields are adopted by authorities within a jurisdiction and across jurisdictions, providing a</p>

NR	REFERENCE IN ACT/BILL/DOCUMENT	COMMENT (Why is it a problem?)	PROPOSED WORDING/COMMENT
			level of commonality, with the remainder of the reporting format tailored to each jurisdiction and/or sector’s regulations and legal frameworks.
4.	Recommendation 4	<p>Phased reporting is vital, but cannot be implemented in isolation from the information requests from authorities</p> <p>Box 1: Examples of information that could be reported to authorities in each CIR phase</p> <p>Initial Report</p> <p>Within South Africa, each FI assesses the severity of the incident in determining whether it is considered material for the affected FI. Only material incidents are then reported to the financial authority. Banks endeavour to provide as much verifiable information as possible when reporting under the 24-hour requirement. The full impact is not always known immediately after detection, so it often takes longer than 24 hours to determine materiality. As soon as a bank classifies an incident as being material, it strives to ensure that its internal governance processes can approve the report to the financial authority within 24 hours and has been able to do so to date. Note that incidents which cross multiple business units take longer to complete review and approvals, so 48 hours would be the recommended change.</p>	<p><b>Recommend</b> a well-defined rule of engagement which both provides authorities with sufficient updates, while giving institutions the space and time they need to deal with a cyber incident while it unfolds and is being responded to so that efforts are focused on incident resolution and recovery to minimise harm, and not on responding to questions from authorities.</p> <p><b>Recommend</b> that reporting timelines changes from 24 to 48 hours</p>
5.	Recommendation 5. Select incident reporting triggers	<p>Due to the nature of cyber incidents, FIs do not always detect an incident as soon as it occurs, sometimes even months later. If reporting were anchored on occurrence date, then Financial Institutions would be in breach for most incidents under the current reporting timelines.</p> <p>Detection date is also challenging from reporting perspective as not much information is known at the time of detection.</p>	<p><b>Recommend</b> supporting the “pre-defined threshold criteria” reporting trigger as the FI then has time to assess the incident and once it reaches the thresholds set, it triggers reporting from that point onwards.</p>

NR	REFERENCE IN ACT/BILL/DOCUMENT	COMMENT (Why is it a problem?)	PROPOSED WORDING/COMMENT
6.	Recommendation 8	<p>In line with the phased reporting cited in recommendation 4, an incident may need to be reported without a full understanding of the extent of the event, and this may both increase or decrease the severity. This provides balance for events that end up hitting thresholds, and for events that are swiftly responded to and prevent thresholds from being breached.</p> <p>South African banks have taken the prudent approach in some cases by reporting to the financial authority on incidents which have the potential of becoming material. South Africa aligns with this suggestion on the basis that this is an informal process as it is currently used.</p>	<p><b>Recommend</b> establishing a common and consistent process to provide initial notification and to both “upgrade” and “downgrade” incidents as they unfold. It is common for an incident to occur that may become material/breach thresholds, and equally so for response and impact mitigation processes to reduce the severity of an event.</p>
7.	Recommendation 9	<p>Effectiveness reviews should not only be isolated to individual institutions. Broader two-way feedback loops are important to enhance systemic resilience.</p>	<p><b>Recommend</b> that authorities provide collective feedback to the sector(s) they regulate, to avoid the common pitfall of one-way information flows from FI to authority.</p>
8.	Recommendation 11	<p>This is dependent on establishing specific, piecemeal cross-sector and cross-jurisdiction agreements.</p>	<p><b>Recommend</b> leveraging existing structures which already bring authorities together such as the BIS.</p>
9.	Recommendation 14	<p>Uncomfortable with the calling out of one body of knowledge regarding incident response (in this case the FSB toolkit).</p> <p>South African banks have implemented robust and reliable structures and processes for identifying, responding, escalating, and reporting incidents, which includes reporting to financial regulators.</p>	<p><b>Recommend</b> making this a more general statement regarding industry-accepted standards or practices (this may include FSB, NIST, or others), and removing the references to specific activities laid out therein.</p>
10.	Recommendation 15	<p>In addition to pooling knowledge, it would be beneficial to provide an online and real-time portal through which the pool of information can be accessed.</p>	<p><b>Recommend</b> the establishment of an information portal to be made accessible for both institutions and authorities.</p>

NR	REFERENCE IN ACT/BILL/DOCUMENT	COMMENT (Why is it a problem?)	PROPOSED WORDING/COMMENT
11.	5.2.1 “Severity rating”	Potentially ambiguous as this can refer both to urgency (how quickly a response is needed) and risk (the level of impact that has materialised e.g., losses incurred).	<b>Clarify</b> whether this seeks to understand urgency response or level of impact, or potentially both. It may be pertinent to include this as part of phased reporting with urgency being more readily identifiable and impact being part of an incident closure and post-incident analysis.
12.	5.2.1 “Services and resources”	While multiple resources may be impacted, disruption to critical services is pertinent from a systemic perspective.	<b>Recommend</b> including the impact on critical/important business services (as defined by BIS in the principles for sound management of operational resilience).
13.	5.2.1 “Impact”	The impact may be both to an individual FI and other stakeholders in the ecosystem	<b>Recommend</b> adding fields to specify the potential impact beyond that on an institution, which can extend to other institutions or roleplays within a sector or financial ecosystem, to provide proactive insight into potential systemic risk.
14.	5.2.1 “Incident closure”	Lessons learned to describe potential control gaps and process improvements needed, but not actual or committed actions from the FI.	<b>Recommend</b> including an optional field(s) for “planned actions” which describe the steps an FI will be taking to action / close gaps from lessons learned.
15.	General	<p>This is a particularly promising idea that can go a long way toward alleviating the regulatory burden in Cyber Incident Reporting. Alignment between the different departments in the SARB (PA, FSCA, Finsurv and PASA) and the ability to use a single reporting interface for all SARB departments will make compliance and communication with the SARB much easier regarding Cyber Incidents. In addition, it could also enhance the SARB’s access to cyber incident data.</p> <p>These principles could even be useful to consider in terms of reporting on other material IT incidents (D2/2019) and cloud computing/ outsourcing arrangements.</p>	<b>Not applicable</b>

NR	REFERENCE IN ACT/BILL/DOCUMENT	COMMENT (Why is it a problem?)	PROPOSED WORDING/COMMENT
16.	Paragraph 5.2 – The FIRE Concept (Pg 28)	The FIRE concept should remain an institution-initiated (push) model, at least in South Africa.	<b>Recommend</b> that the SARB/ PA should clarify/ provide additional guidance as to the interpretation of the “materiality” concept in Directive 2/2019 to better guide the level of reporting expected from FIs. However, it should not have access to all Cyber Incident data/ alerts generated by SOCs (as could be the case in a pull model) as this could create a lot of noise
17.	Page 5 Main Incident Report Framework	Does not consider the frameworks or reporting requirements outside the EU	<b>Clarify</b> how this aligns with African regulators.
18.	Page 8- Setting reporting criteria challenges. Second, there is a potential for a lack of common understanding of 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 in reporting	In support of the point made that due to various regulatory bodies the reporting requirements are not always consistent.	<b>Support</b>
19.	Page 23 Authorities can decide the extent to which they wish to adopt	Important that this statement remains true, as we have various financial regulators at various levels of maturity.	<b>Support</b>

NR	REFERENCE IN ACT/BILL/DOCUMENT	COMMENT (Why is it a problem?)	PROPOSED WORDING/COMMENT
	<p>FIRE, if at all, based on their individual circumstances. For instance, authorities could consider leveraging a subset of the features or definitions, which would promote a limited form of convergence. Even if not adopted by a single jurisdiction, it could still serve as a common baseline for FIs to map against a range of reporting requirements and assist in translating between existing frameworks.</p>	<p>This should be seen as a mechanism to assist financial institutions and not become a governance function</p>	
20.	<p>General</p>	<p>The document has a lot of European slants probably because of the maturity level of the CSIRTs on the continent. The implication is just that continental realities might be missed. I think Juan will be in a better position to provide valuable comments.</p>	<p><b>Recommend</b> that a linguistics team review the document to ensure the readability of the standard can be correctly interpreted and referenced in the South African context.</p>
21.	<p>2.3 Culture of timely reporting</p>	<p>There also needs to be considered that culture is also underlying recent technologies used that would require longer route cause analysis for accurate reporting. This will not be covered under inadequate capabilities and some capabilities can only be developed once recent technology threats materialised and reversed engineered.</p> <p>Unfamiliar technologies and strategies would also lead to delayed reporting due to more extensive RCAs.</p>	<p><b>Recommend</b> that the culture underlying recent technologies, be considered.</p>
22.	<p>General</p>	<p>The document is written on the premise that the target market has reached a certain level of high maturity. The implementation and operationalisation of this will be evaluated when compared to well-established markets with a readily available educated resource pool.</p>	<p><b>Recommend</b> considering the applicability to the society it is targeting as maturity and culture plays a significant part when having to implement CIR and the effectiveness thereof. It also needs to consider the diverse size of organisations and their ability to operate in this sector.</p>

NR	REFERENCE IN ACT/BILL/DOCUMENT	COMMENT (Why is it a problem?)	PROPOSED WORDING/COMMENT
23.	Common terminologies for CIR	<p>Phishing</p> <p>Does every phishing attempt pretend to be from a trustworthy source? A person can be phished without the attacker pretending to be from a trustworthy source e.g. "You have won an Apple iPhone 14 in our random draw. Please register your details here to claim your prize."</p> <p>Ransomware</p> <p>Use may continue to be impaired even after the ransom demand is satisfied, or when the victim chooses not to accede to the ransom demand.</p>	<p>Clarify</p> <p><b>Recommend</b> removing "until a ransom demand is satisfied."</p>
24.	Common terminologies for CIR (Section 4)	<p>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?</p>	<p><b>Yes</b>, the revised Lexicon is going to enable consistency and promote the adoption of a common reporting format in the industry.</p> <p>While the changes do promote a common understanding of the cyber-related terms, there is further clarity required.</p>
25.	Common terminologies for CIR (Section 4)	<p>Do you agree with the definition of 'cyber incident,' which broadly includes all adverse events, whether malicious, negligent, or accidental?</p>	<p><b>Yes</b>, agreed that these are: Cyber events causing a financial or non-financial impact on an organisation, committed by internal or external threat actors whether malicious or otherwise.</p> <p>Cyber is primarily an attacker-oriented risk (malicious). A negligent or accidental data leakage/system unavailability may be classified as an information risk, or a technology change risk (separate Non-Financial Risk types) as opposed to a cyber incident. There needs to be clarity in the definition to highlight the difference or overlap between cyber, information, technology change and privacy incidents</p>



NR	REFERENCE IN ACT/BILL/DOCUMENT	COMMENT (Why is it a problem?)	PROPOSED WORDING/COMMENT
26.	Common terminologies for CIR (Section 4)	Are there other terms that should be included in the Cyber Lexicon to cover CIR activities?	No
27.	Common terminologies for CIR (Section 4)	Are there other definitions that need to be clarified to support CIR?	<p>Cyber-attack - An attack, via cyberspace, targeting an enterprise's use of cyberspace for the malicious purpose of causing loss, disrupting, disabling, destroying, or controlling a computing environment/infrastructure; or destroying the confidentiality, integrity, and availability of the data.</p> <p>Cyber event - Any act or attempt, successful or unsuccessful, to gain unauthorized access to, disrupt or misuse an Information System or information stored on such Information System.</p>
28.	Format for Incident Reporting Exchange (FIRE) (Section 5)	Would the FIRE concept, if developed and sufficiently adapted, usefully contribute towards greater convergence in incident reporting?	<b>Support</b> the opportunity to drive convergence and standardisation, with care being taken to ensure that this does not become onerous on the FI.
29.	Format for Incident Reporting Exchange (FIRE) (Section 5)	Is FIRE readily understood? If not, what additional information would be helpful?	<b>Yes</b>
30.	Format for Incident Reporting Exchange (FIRE) (Section 5)	If FIRE is pursued, what types of organisations (other than FIs) do you think would need to be involved?	<b>Technology</b> Service Providers, <b>Telecom</b> companies.
31.	Format for Incident Reporting Exchange (FIRE) (Section 5)	What preconditions would be necessary to commence the development of FIRE?	<b>Flexibility</b> for implementation by the local regulator. Consider integration via the existing local regulatory requirements for incident reporting, as opposed to introducing an additional set of requirements.

NR	REFERENCE IN ACT/BILL/DOCUMENT	COMMENT (Why is it a problem?)	PROPOSED WORDING/COMMENT
			Wider industry adoption of the Cyber Lexicon and common understanding of a cyber incident and materiality
32.	Operational Challenges	<p>The requirement to notify the regulator within 24 hours of recognising a material incident does impact the operational teams responding to and remediating the incident as these are often the same resources that have the information required for assessing whether the material is considered material, as well as providing the information required for reporting.</p> <p>A cyber incident could also have other ramifications e.g., Personal Information data breaches which then require the FI to report such incidents to the Information Regulator as well, with a diverse set of reporting and timeline requirements. It initiates multiple independent and concurrent streams of reporting, for which the source of the information is the operational teams dealing with the incident.</p> <p>Criteria for determining materiality for cyber and personal Information data breach incidents are different which increases the complexity of assessing the materiality of an incident where it spans both. Incident Templates for reporting are also different.</p> <p>Each FI has established its own set of criteria for assessing materiality. Often, client messaging of issues on social media generates incident information requests from the relevant regulator, even though the incident was not considered material. Whilst banks accept the right to request such information from the regulator, it does create additional operational impact in providing such a response.</p>	<b>Recommend</b> that 48 hours would be more appropriate to ensure that a more complete set of information is provided, as well as allow for internal governance and reviews, especially where such incidents impact multiple business units across the group.

NR	REFERENCE IN ACT/BILL/DOCUMENT	COMMENT (Why is it a problem?)	PROPOSED WORDING/COMMENT
		<p>Local banks have managed to comply with the 24-hour reporting timeline for material incidents. It must be noted that often, not much information may be available during the first few (and 24 hours) of an incident to enable accurate assessments of materiality. Therefore, ensuring completeness of information and accuracy of reporting in respect of the information required in the 24-hour reporting template often proves challenging to meet the timeline for reporting</p>	
33.	Early assessment challenges	<p>The root cause is not normally confirmed within 24 hours of an incident; however, this is compulsory information in the 24-hour reporting timeline. The root cause is also not always confirmed within the 14-day required timeline and can often take months to do so, especially where vendor support is required. However, banks do appreciate that the regulators understand this issue well, and often accommodate requests for delayed reporting of the root cause.</p>	
34.	Recommendations (Section 3)	<p>Can you provide examples of how some of the practical issues with collecting and using cyber incident information have been addressed at your institution?</p>	<p>In the South African context, the local central bank has already issued a guidance note in this regard which helped to deal with some of the challenges stated in the FSB consultative paper. Accordingly, banks have used the requirements of the guidance note to define internal and internal processes, and a reporting template as well as allocate responsibilities for collating incident information for reporting.</p>
35.	Recommendations (Section 3)	<p>Are there other recommendations that could help promote greater convergence in CIR?</p>	<p>Closer alignment between regulatory requirements and legislative requirements (e.g., Privacy reporting)</p>

NR	REFERENCE IN ACT/BILL/DOCUMENT	COMMENT (Why is it a problem?)	PROPOSED WORDING/COMMENT
36.		Are there other recommendations that could help promote greater convergence in CIR?	Closer alignment between regulatory requirements and legislative requirements (e.g., Privacy reporting)
37.		Could the recommendations be revised to address the identified challenges more effectively to achieve greater convergence in CIR?	No