National Bank of Belgium

We'd like to thank you for the opportunity to provide you with feedback on the consultative document on "Effective Practices for Cyber Incident Response and Recovery". Even though we are very supportive of the content of this document, we have the following questions/suggestions/remarks:

- What will be the status of the final "toolkit" document? To what extent is there a formal expectation that financial institutions and financial market infrastructures will (fully) align with these "good/best practices"? Maybe this can be indicated more clearly in the document?
- Governance section: Box 1 - metrics: "volume" of customers impacted and "volume" of incidents: Is there a difference or a nuance in meaning between "volume" and "number"?
- Preparation section:
    - "Stress tests" -> Is there already an industry-wide common understanding of this concept? Or would it be desirable to further clarify/define this concept?
    - "They implement commercially off-the-shelf technology solutions …" -> Usually, we try to be technology agnostic in our supervisory expectations or regulatory documents. Is the mentioning of "commercially off-the-shelf technology solutions" essential in this paragraph?
- Analysis section: Box 3 – Information to be used when describing cyber incidents -> We believe that the "intent" and the "threat actor" are 2 dimensions of an incident that are not always possible to identify. Even if it is possible, we notice in some cases some reluctance to share this information (even with the supervisor/regulator). Of course, this does not mean that these concepts could not be part of a CIRR taxonomy.