Central Bank of Hungary

First of all, it is important to highlight that this consultative document is really useful and timely as cyber incident response and recovery is getting a more and more important issue after the Covid crisis, when the secure and effective operation of the digital services and solutions and the fast incident handling and recovery are becoming more essential for everyone.

This toolkit is really detailed and mentioning all of the important steps/ elements of incident analysis, response and recovery.

The present document is a huge collection of possibilities for the financial institutions, but it does not provide any guidance on what are the essential elements on which to build the other useful optional tools.

According our views, it would be important to emphasize the existing international/EU requirements for incident handling and reporting (PSD2, NIS directive, EBA ICT gl.;GDPR etc.), to see the common minimum elements that most of the undertakings must comply with.

We fully support the idea presented in the virtual meeting on 9th of July, to add a maturity level assessment (questionnaire/guide) as an annex, to help the institutions to identify their maturity and to identify the areas that need to be further developed (by any tool from the toolbox).

Finally, maybe a little more emphasis could be placed on incident reporting requirement to the authority(s), as it is important to establish the process, identify the responsible person etc.