Verband der Auslandsbanken in Deutschland e.V.
Association of Foreign Banks in Germany

EBA
One Canada Square (Floor 46)
Canary Wharf
London E14 5AA
UK

March 13, 2019

Consultation ICT Guidelines

Dear Sir or Madam,

We thank you for the opportunity to comment on the draft of the EBA Guidelines on ICT and security risk management

The Association of Foreign Banks in Germany represents the interests of currently more than 200 foreign banks and other financial services institutions which operate in Germany via subsidiary or branch.

Our Members' business models are very diverse. Among the member firms there are globally and internationally active banks of a larger scale as well as smaller institutions with focus of certain business areas (limited business model). However, all have in common that they operate cross border and use the IT infrastructure and services the group provides in order to streamline costs and work efficiently both internally and for the clients. In order to reach this, especially the parent entities of such a cross-border group support and provide their branches and subsidiaries (in different host Member States) with IT functions, know-how, BCM measures, etc. In the light of this setup we comment on the draft.

In general, we appreciate the creation of harmonised rules on Level 3, as almost all member institutions are part of a cross-border banking group. Those banking groups benefit from a regulatory level playing field arising from the harmonisation of financial sector regulations within the European Union.

With regards to the following points, we would like to share our thoughts with you:

Elke Weppner

Association of Foreign Banks in Germany
Weißfrauenstraße 12-16
60311 Frankfurt am Main
Germany
Tel: +49 69 975850 0
Fax: +49 69 975850 10
elke.weppner@vab.de
www.vab.de

Guideline 4.2. ICT governance and strategy

Section 4.2.3. Use of third party providers

Although no prejudice to the coming EBA Guidelines on outsourcing arrangements (EBA GL 2019/XX) and Article 19 PSD2, it is said in marginal number 7 that financial institutions should ensure that contracts and service level agreements have to be arranged even for outsourcing to group entities. In general, we would prefer a clear alignment with the requirements set out in the EBA GL 2019/XX on outsourcing arrangements. However, it remains unclear if it is necessary to differentiate between parent entities based in another Member State and parent entities in a third country.

Guideline 4.3. ICT risk management framework

Section 4.3.1. Organisation and objectives

- In marginal number 11, the Guidelines describe a three lines of defence model in which the internal control function acts as a second line of defence. In this context, the final Guidelines should clarify that this internal control function can be organisationally situated outside of the IT department in order to ensure independency and avoiding conflicts of interests.

- Furthermore, in marginal number 11 remains unclear what is meant with *"where the three lines of defence model is applied"*. In marginal number 10 it is stated as a mandatory requirement to manage the ICT risk according to the three lines of defence model whereas marginal number 11 seems to leave it open to not manage the ICT risks under this model using the term "where the three lines of defence is applied". Clarification is therefore necessary. However, we would welcome a wording which suggests the three lines of defence model but due to reason of proportionality, respectively in small financial institutions, risk management can be done as effectively as necessary under a different approach but the three lines of defence model. It should be more important to create a robust ICT risk management with an independent internal control function than to formally stick to a model. This approach would be especially valuable in situations where due to head count the implementation of all three lines would proof to be difficult.

Guideline 4.4. Information security

Section 4.4.3. Logical security

- In lit. (d) of marginal number 34, there is a hint on retention requirements set out in EU and national law with regards to the period of time of retaining access logs. It should be

clarified, that the data safeguards requirements should be in line with other regulations which give guidance on retention periods on EU level, i. e. GDPR.

- As one measure to secure a robust ICT risk management within financial institutions the position of an information security officer can be foreseen. We interpret marginal number 32 more as a function which can be carried out by a team representing the information security function as second line of defence; it should not necessarily mean the appointment of an information security officer. As for that it should be clarified that with the appointment of an information security officer the information security function is established. According to proportionality it may be necessary for the information security officer to have a team but this should be a question of size and risk exposure of the individual financial institution.

Guideline 4.5. ICT Operations management

- In marginal number 55 the draft requests documentation of approved procedures. However, the way of how documentation and maintenance of such documentation is done is quite different in the financial institutions. Either way, the guidelines should leave room for individual documentation in order to avoid additional bureaucratic burden for resources.

- It should also be clarified that only material changes in the overall ICT risk management documentation should be approved by the management body since not every tiny change and adaption needs management approval as long as the overall concept is not changed.

Guideline 4.7. Business continuity management

Section 4.7.3. Response and recovery plans

Regarding the BCM measures, it should be sufficient from a host NCA perspective that BCM measures could also be implemented by the parent entity of a cross-border group if the parent entity is situated in an EU Member State. Further, guidance is needed with regard to BCM measures provided by parent entities in third countries. We suggest aligning this with the supervisory equivalence decisions which allow that as equivalent recognised countries are treated similar to Member States.

Guideline 4.8. Payment service user relationship management

The Guidelines set out in marginal number 103 that PSPs should keep payment service users (PSUs) informed about updates in security procedures which affect PSUs regarding the provision of payment services. In addition, it is said marginal number 104 that PSPs should provide PSUs with assistance on all questions, requests for support and notifications of

anomalies or issues regarding security matters related to payment services. In this context, there is no differentiation made between PSUs that are consumers and payment service users that are corporate clients. With regards to corporate clients, PSPs could expect a more elaborated knowledge and understanding of risks and threats related to payment services in comparison to PSUs that are consumers. It should be appropriate to amend a risk-based approach to these provisions in order to enable differentiated treatment of PSUs with regards to the scope of information needed.

It would be appreciated if the above suggestions are taken into account in the future elaboration of these guidelines. We have no objections to the disclosure of our comments.

Kind regards,

Dr. Oliver Wagner Elke Weppner Andreas Kastl