With regard to the Consultation Paper on Guidelines on ICT and Security Risk Management we would like to submit the following comments on all proposals put forward in the above mentioned document:

Section 4.2.3. Use of third party providers

PT 7. We would like to suggest making the following amendments:

"Without prejudice to the EBA Guidelines on outsourcing arrangements (EBA GL 2019/XX) and Article 19 PSD2 financial institutions should ensure the effectiveness of the risk mitigating measures as defined by their risk management framework, including the measures set out in these Guidelines, when important operational functions of payment services and/or ICT services and ICT systems, are outsourced, including to group entities~~, or when using third parties~~."

- Comment: The fact of providing services by third parties in their own account shouldn't cause a duty to practise EBA Guidelines on outsourcing arrangements.

Section 4.3.1 Organization and objectives (ICT risk management framework)

PT 10. *Financial institutions should identify and manage their ICT risks according to the* ***three lines of defence model****.*

- Comment: Three lines of defence requirement can be difficult to be met by smaller companies as they may not have enough people with adequate technical skills and InfoSec background outside of ICT support teams (second line)

PT 13. *Risk management framework should include processes in place to:*

a) determine the risk tolerance, in accordance with the risk tolerance of financial institutions;

- Comment: 'Risk tolerance' is rather a term used in connection with the investments whereas the whole document is rather about ICT-related risks (technology-related). Wouldn't be reasonable to provide in the definition of the term some more details relating to ICT issue?

b) identify and assess the ICT risks to which financial institutions are exposed;

- Comment: We would like to suggest providing a short definition of what the risk of financial institution tolerance is (whether is it an acceptable level of product/multiplication of probability*impact of a given risk?). It would be also good to provide, as a guideline, a list of common risks that should/must be considered in risk assessment/risk mitigation process, which are, for instance:

* unavailability of key stuff of financial institution

* unavailability of data centre facility (fire, power outage, power from city grid unavailable for 4,8, 24h)

* cyberattack (DDoS, ransomware)

* data leakage (inside job, external attack)

(Some of the risks are listed in paragraph 39 - 3.2.1 review of the institutions's ICT risk profile in EBA/GL/2017/05)

Section 4.5 ICT operations management

PT 64. *Financial should establish and implement an incident and problem management process to monitor and log operational and security ICT incidents and enable financial institutions to continue or resume critical business functions and processes when disruptions occur. Financial institutions should determine appropriate criteria and thresholds for classifying an event as an operational or security incident, as set out in the 'Definitions' section of these Guidelines, as well as early warning indicators that should serve as an alert to enable early detection of these incidents.*

- Comment: in the first line there might be a word 'institutions' missing:
  current wording: 'financial should establish…'
  our proposal: financial institutions should establish…'

section 4.6.1 ICT project management

PT 66. *Financial institutions should implement a governance process with an adequate project implementation leadership to effectively support the implementation of the ICT strategy through ICT projects.*

- Comment: the term '*adequate project implementation leadership*' sounds pretty vague, wouldn't be reasonable to provide some clarification of this term?

PT 68. *Financial institutions should establish and implement an ICT project management policy which defines the phases of each project and includes at a minimum:*

a) project objectives; b) roles and responsibilities; c) project risk assessment; d) project plan, timeframe and steps; e) procurement management; f) key milestones; g) and change management requirements.

- Comment: Some financial institutions may use agile project management approach, which, due to its nature, may not meet all requirements indicated in PT 68.

Section 4.7.4 Testing of plans

PT 95a. *Financial institutions' testing of their BCPs should demonstrate that they are able to sustain the viability of the business until critical operations are re-established. In particular they should:*

a) include an adequate set of severe but plausible testing scenarios including those considered for the development of the BCPs (including testing of services provided by third parties, where applicable). This should include the switch-over of critical business functions, supporting processes and information assets to the disaster recovery environment and demonstrating that it can run them for a sufficiently representative period of time, and that it can restore normal functioning afterwards

- Comment: suggests that redundant infrastructure (servers, data centre) must be implemented - requirement to have such infrastructure at those levels should be a result of Business Impact Analysis, risk assessment analysis and Recovery Time Objective parameter defined and the ability of financial institution to recover services within Recovery Time Objective time. If Recovery Time Objective does not exceed the maximum time and financial institution is able to recover its services to normal operations in their primary location, then an extra recovery environment may not be required.

PT 98. *PSP should establish and implement processes to enhance PSU's (payment services user) awareness of security risks linked to the payment services by providing PSUs with assistance and guidance*

Comment: Is it a consent of PSU required to send such awareness info (campaigns, bulletins, etc)