European Banking Authority
One Canada Square (Floor 46)
Canary Wharf
London E14 5AA

13 March 2019

(Submitted via online form)

Dear Sir/Madam,

Standard Chartered's response to the European Banking Authority's (EBA) Consultation Paper on draft Guidelines on ICT and security risk management (EBA/CP/2018/15).

Standard Chartered invests significant sums to maintain the security and effectiveness of our existing ICT estate. We are continuously overseeing our information security policy as well as our risk control framework, training procedures and ICT governance in general.

We strongly support efforts to align the requirements applicable to ICT and security risks across existing EU regulations. Ensuring a level playing field with consistent requirements applicable to credit institutions and payment services institutions with those of investment firms will provide certainty on the regulatory environment that institutions operate within.

As an international bank with operations across several continents we also believe it is of fundamental importance to as far as possible strive for international harmonization of stringent rules in the ICT area, not only within the European Union but globally as well. Diverging regulatory requirements will significantly increase operating costs as well as introduce risks of regulatory arbitrage.

Technological development in the ICT area is rapid and we believe it is important that guidelines be principles based and sufficiently flexible to accommodate innovation.

We thus recommend that the EBA gives further consideration to the following aspects which we believe to be of importance:

Principles Based

SCB welcomes that the guidelines are, in general, principles based. We believe that this is essential and should be maintained as far as possible. A focus on outcomes and how firms can demonstrate capabilities increases consistency and alignment between jurisdictions and ensures that the guidelines can be implemented with proportionality in mind. In addition, the principles based approach should incorporate the notion of materiality. To illustrate: Only information assets, which when not available would cause a significant business loss, should be required to be mapped.

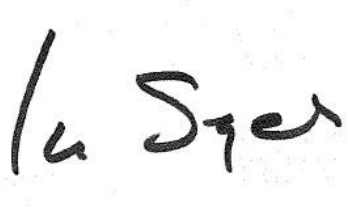
Alignment across jurisdictions

Departure from existing recognized standards increases regulatory complexity and requires resources to be diverted from other activities. This inhibits firms to focus efforts on the identification and protection against technological risks, thus increasing firms' resources focusing on compliance rather than technological security.

Standard Chartered Bank
1 Basinghall Avenue
London EC2V 5DD
Tel +44 (0)20 7885 8888
www.standardchartered.com

We hope these comments are helpful, and we would be pleased to discuss our views with you in greater detail.

Yours sincerely,



Ian Sayers
Global Head, Group Regulatory Liaison and Acting Global Head, Regulatory Reform Compliance

Annex: Comments to the consultation paper sections

Subject matter, scope and definitions (pages 12-14)

- EBA should consider reviewing the definition for "Operational or security incident'. A singular or series of unplanned events which 'will probably' have an adverse impact is a risk, and not an operational or security incident. SCB recommends that EBA align as far as possible definitions with international publications on technology and cybersecurity risks such as the FSB Cyber Lexicon.

4.2. ICT Governance and strategy (page 15)

- SCB wishes to see clear lines of responsibility and accountability between the management board and senior management. The accountability of the Board should focus on setting the firm's risk strategy/appetite, and the ability to challenge decisions of the ICT functions. We recommend Board responsibilities to be amended in the guidelines (in paragraph 4) to permit delegation where deemed adequate, for instance where it is expected from the management body to implement processes. The need for the management body to approve specific risk type policies should also be reconsidered.

- EBA's guidelines on outsourcing arrangements are expected to be published soon. For section 4.2.3, we suggest that the ICT risk management guidelines refer directly to EBA's guidelines on outsourcing arrangements. Accordingly, paragraph 8 and 9 can be dropped.

4.3. ICT Risk Management Framework (pages 16-19)

- SCB fully appreciates the need for firms to update its ICT risk management framework with "lessons learned" (paragraph 14). However, the way firms decide to do this may vary. We seek clarification on the implementation of such a continuous improvement process. As the point is subject to different interpretations as 'lessons learned' documentation could be inferred as part of the project closure documentation or the lessons learned from ICT incidents and outages. Additionally, we request clarification on the level of documentation and the level of criticality of the incidents that should be captured in the 'lessons learned' documentation.

- To ensure consistency when referring to ICT organization structure, we suggest paragraph 12 in section 4.3.1 be amended to align with section 4.2.1 and section 4.3.2 to include any interdependencies to ICT risks within the organization. We suggest amending paragraph 12 to "this framework should be fully integrated into, and aligned with, financial institutions' overall risk management processes including any interdependencies related to the ICT risk".

- We suggest that a guidance for risk tolerance (thresholds) be specified in regards to section 4.3.2 (identification of functions, processes and assets). The requirement should be limited to mapping business functions, roles and processes which would lead to a critical or significant ICT risk based on acceptable risk thresholds.

- Regarding such thresholds, we recommend that in paragraph 17 only information assets, which when not available would cause a significant client or sector impact, should be required to be mapped. Similar to our feedback on the previous point on mapping functions, processes and assets, the principle of proportionality and guidance for risk tolerance should be followed.

4.4. Information security (pages 19-23)

- We recommend that section on logical security, paragraph 34 (d), specify what type of privileged user activities should be logged. The objective should be logging of exception activities (e.g. failed logons, reconciliation breaks) and should distinguish between interactive and non-interactive privileged activities.

- We recommend that security monitoring (paragraph 42) should be rephrased to state that financial institutions establish a threat intelligence gathering and assessment process to identify, triage and counter targeted threats, and that this is embedded into its log correlation and orchestration processes. Firms should know what they are monitoring against.

4.5. ICT Operations Management (pages 24-25)

- SCB recommends that the requirements as regards ICT systems and data backups and restoration procedures (paragraph 62) remain principle based. Back up requirements should be aligned to the business recovery requirements. System criticality is more aligned to the Business Impact Assessment for Technology under Business Continuity Management.

4.7. Business continuity Management (pages 28-30)

- Financial institutions are reliant on third party service providers including Financial Market Infrastructures (FMIs) such as payment, clearing and settlement operators to ensure continuity of services to the customer. FMIs are subject to regulatory requirements for their resilience framework (such as the ECB's Cyber Resilience Oversight Guidance for FMIs or the Principles for FMIs issued by Bank for International Settlements (BIS) and International Organization of Securities Commissions (IOSCO)). However, it is not always within the control of an individual bank or financial institution to mandate or ensure compliance of FMIs business continuity planning or testing its response and recovery capabilities.

  Although FMIs are a subset of the bank's interdependencies, we recommend that section 4.7 (including paragraphs 93 to 95) caveats the guidelines with an appropriate qualifying statement to exempt bank from the responsibility of FMIs business continuity planning and ongoing BCM governance.