HSBC

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

21 December 2016

Dear Sir/Madam

Response to the EBA Consultation Paper: Guidelines on ICT Risk Assessment under the Supervisory Review and Evaluation process (SREP)

Introduction

HSBC welcomes the opportunity to express our views on the **"Guidelines on ICT Risk Assessment under the SREP"** (EBA-CP-2016-14) issued on 6 October 2016.

Our Observations

Information and Communication Technology (ICT) and associated risks are continuously evolving within the global financial services industry and we have noted the regulators' increasing focus on this area.

We therefore welcome the publication of this Consultation Paper (CP) by the EBA and the drive towards harmonisation of practices across National Competent Authorities (NCAs) and financial institutions. Notwithstanding this, we view these risks as operational risks and as such we believe they should be managed and controlled as part of an integrated risk framework which is aligned to existing guidance such as the Principles of Sound Management of Operational Risk.

We believe that this CP seems to provide a sound basis for the assessment of ICT risks. We are therefore, in principle, supportive of its objectives. As part of this response, we would take this opportunity to provide our high-level observations on this CP and seek additional clarifications from the EBA.

Having reviewed the CP in detail, and having participated in the public consultation exercise, below are our key general and specific observations:

General Observations:

- **Explicit identification of expectations of financial institutions**

It is clear that these guidelines are aimed at guiding NCAs in better assessing ICT Risks as part of the SREP process. We also note that Page 10 Paragraph 1 states that *"...competent authorities and financial institutions must make every effort to comply with the guidelines"*. It is not clear within the CP which elements are requirements that supervised financial institutions are specifically expected to adopt; clarification in the final Guidelines will be welcomed.

Continued...

- **Consistency of Regulatory Standards**

We understand that the US regulators are in the process of producing enhanced regulatory standards on Cyber Security which may overlap with aspects of the Guidelines. Where possible, the EBA should ensure that European and US standards are aligned and not potentially contradictory. This is of particular importance for a global banking group such as HSBC.

Specific Observations:

- **Classification of ICT change and ICT outsourcing as independent risk types**

  Within the identified risk types there are classifications of ICT change risk and ICT outsourcing risk. On the basis that these risk classifications relate to the support and delivery of systems and data, both internally and externally, we believe these are **causes** of three principle risks (confidentiality, integrity or availability) **rather than separate, quantifiable risks** in their own right. This is illustrated below:

  - **Change risk**

    - Incorrect change or delivery of a system would result in the system not meeting operational standards leading to the risk of unavailability;
    - Incorrect changes to the data that flows through the system would lead to a risk of the date integrity and possibly the data availability; and
    - Incorrect changes to the security parameters of the system as a result of change would lead to a risk in terms of the confidentiality, integrity or availability of the system.

  - **Outsourcing risk**

    - Failure within a third party solution would crystalize as a breach of confidentiality, a corruption of systems or data, and/or the unavailability of the system. HSBC sees these as the primary risks to manage. The introduction of an outsourcing risk would be duplicative and therefore redundant as the effect on the three primary risks still needs to be considered.

Therefore, we aim to continue to assess our risk profile on the basis of our current approach to assess confidentiality, integrity and availability risks, which already captures ICT change and outsourcing risks.

During the public consultation, it was made clear to the audience that the adoption of the CP's ICT risk taxonomy is not mandatory for supervised financial institutions. A statement in the final Guidelines confirming this would be welcomed.

- **Scoring under EBA SREP Guidelines**

  - We understand that the ICT risk assessment will contribute to the overall SREP assessment in a range of ways. The assessment of governance and strategy for ICT would feed into the assessment of internal governance controls (under Title 5 of the EBA SREP guidelines) and potentially inform the assessment of the business model (under Title 4 of the EBA SREP guidelines). In addition, the assessment of ICT risk will inform the Operational Risk Score for the institution (under Title 6 of the EBA SREP guidelines).

Continued...

- We are therefore concerned that there may be potential for duplication in the scores that are awarded to an institution under various sections of the EBA SREP guidelines. Different supervisory teams or individuals may assess the institutions' ICT risks from various perspectives and may end up 'double counting' risks.
- We would welcome further clarification from the EBA on these issues and how the ICT risk assessment may inform an institution's final SREP score.

- **Stress Testing and Capital Quantification**
  - We would welcome further clarity in relation to the manner in which the supervisory assessment is expected to lead to capital requirements for Operational Risk. The Guidelines currently provide the overarching requirements to assess ICT risks. However, they stop short of providing transparency in relation to the capital impact of the assessment.
  - For example, Paragraph 29 of the Guidelines seems to suggest that internal capital would be assessed in relation to *"...expected and adverse scenarios, e.g. scenarios included in the institution-specific or supervisory stress test."* Does this mean that supervisors (and institutions) are expected to assess ICT risks from a macro-economic stress test (Pillar 2B in the UK) perspective?
  - We would welcome additional transparency in this matter (similar to that provided by the Prudential Regulation Authority in the UK through Policy Statement 17/15).

- **Role of Second and Third Lines of Defence**
  - We welcome the emphasis on robust management oversight. The guidelines also recommend the possible use of Internal Audit (third line of defence) for assurance purposes.
  - In this context, further clarity in the final Guidelines regarding expectations of a second line of defence would be beneficial. For global banking groups, this would make it clear whether the EBA's expectations are aligned with the recent OCC/Federal Reserve proposals on Enhanced Cyber Risk Management Standards which articulate regulatory expectations of both second and third lines.

Conclusion

HSBC welcomes the introduction of these Guidelines as they will lead to greater transparency for NCAs and supervised financial institutions of the materiality associated with ICT risk across the industry. We believe further consideration and clarity of these Guidelines is required to assist financial institutions to understand what additional requirements (if any) this introduces.

We do hope the EBA finds this letter helpful. We are committed to helping in whatever way we can to build upon the results of this CP. Please do not hesitate to contact me should you wish to discuss matters raised in this submission.

Yours faithfully

Mark Cooke
Global Head of Operational Risk