Deutsche Börse Group
Response

to EBA/CP/2018/15

"EBA draft Guidelines on ICT and security risk management"

published for consultation on 13 December 2018

Eschborn, 13 March 2019

Contact: Marija Kozica
Telephone: +49 (0) 69 211 - 17178
Telefax: +49 (0) 69 211 - 13315
Email: marija.kozica@deutsche-boerse.com

A. Introduction

Deutsche Börse Group (DBG) welcomes the opportunity to comment on 'EBA draft Guidelines on ICT and security risk management' published for consultation on 13 December 2018 (in the following (EBA) draft guidelines).

DBG operates in the area of financial markets along the complete chain of trading, clearing, settlement and custody for securities, derivatives and other financial instruments and acts as such as a provider of highly regulated financial market infrastructures.

Among others, Clearstream Banking S.A., Luxembourg and Clearstream Banking AG, Frankfurt/Main, acting as (I)CSD[1], as well as Eurex Clearing AG as a leading European Central Counterparty (CCP), are authorized as credit institutions within the meaning of point 1 of Article 4 (1) of the Capital Requirements Regulation (CRR). Moreover, the Clearstream subgroup is supervised on a consolidated level as a financial holding group while in addition, Eurex Repo GmbH and 360 Treasury Systems AG are operators of multilateral trading facilities (MTFs) and classify as CRR investment firms according to point 2 lit. c of Article 4 (1) CRR. Authorised as institutions within the meaning of point 3 of Article 4 (1) CRR, the aforementioned entities of DBG fall within the scope of these draft guidelines.

The importance of information and communication technologies (ICT) for the provision of financial services to our clients is steadily increasing, not only for the institutions in our group being within the scope of the draft guidelines, but also for other group entities (including operators of regulated markets). DBG has built its trading facilities as well as its clearing and settlement services on the continuous development of reliable state-of-the-art technology, thereby contributing to the safety and integrity of financial market. As such, DBG relies on a profound, secure and resilient ICT-architecture, embedded in a comprehensive risk management framework steadily enhancing resilience to handle emerging ICT-related risks.

While we welcome EBA's intention to contribute to a better understanding of supervisory expectations and harmonisation of requirements across different financial entities within the EU, we are of the opinion that some of the requirements are inexpedient or potentially not fit for purpose whereas others need further clarification.

The document at hand contains our general comments to the draft guidelines on ICT and security risk management (Part B) as well as dedicated remarks on selected requirements (Part C).

B. General comments

Particularly in view of the increasing importance of ICT systems and services for internal processes but also for the provision of financial services to clients across entities, it is our belief that a robust and resilient framework for managing ICT and security risks is of utmost importance. With growing reliance on ICT systems and services together with increasing exposure to emerging ICT risks affecting entities irrespective of their supervisory status, issuance of clear and comprehensive guidelines on

[1] (International) Central Securities Depository

ICT risk is highly appreciated. Against this background, we support EBAs approach to develop guidelines on ICT risks applicable to PSPs as well as to credit institutions and investment firms likewise.

Regardless of our general consensus with the draft guidelines provided, we consider some selected requirements of the draft guidelines as expendable and not fit for purpose. Particularly, Chapter 4.6 "ICT Project and Change management" outlining guidelines on the implementation of ICT related changes primarily through a project setup, lack clear insight on state of the art ICT challenges. While we generally appreciate clarification of supervisory expectations on ICT change management and acknowledge the importance thereof, we are of the opinion that the draft guidelines focus too strongly on a project setup, which does not fit the actual practice in, among others, software development. Software is increasingly being developed continuously or in agile project setups (e.g. SCRUM) rather than in so called "waterfall" project setups (as particularly indicated under paragraph 68 of the draft guidelines). We are of the opinion, that the EBA guidelines on ICT Project and Change management should therefore rather focus on providing clarification on supervisory expectations regarding an adequate governance and control structure related to (material) changes. Furthermore, the draft guidelines on ICT project management, as specified under Chapter 4.6.1 of the draft guidelines, do not contain any ICT related specifications but constitute general requirements on project management applicable to a multitude of fields and should therefore be incorporated (including agile project setups) in guidelines rather focusing on institutions' organisational duties. One possibility would be to include the draft guidelines on ICT project management, as general requirements on e.g. project and change management, into the Guidelines on internal governance under Directive 2013/36/EU (EBA/GL/2017/11).

While we fully support the principle of proportionality and regard flexibility in assessing the adequacy of governance structures, controls and further measures as of high importance, we would highly appreciate clarifying references to existing and generally acceptable standards (e.g. reference to ISO 27001/2 for controls and ISO 27005 for risk management), where appropriate. We belief that references to existing standards will ease harmonisation across member states and provide assistance in consistent interpretation of requirements. Moreover, we would appreciate additional clarification on specific aspects of the guidelines in order to harmonise implementation of requirements further and ensure an appropriate application of rules, which we outline further below as part of our comments on selected paragraphs.

In May 2017, EBA published Guidelines on ICT Risk Assessment under the Supervisory Review and Evaluation Process (EBA/GL/2017/05) providing guidance on assessing a variety of fields related to ICT risk, like identification of material ICT risks and assessment of controls for mitigating ICT risk. Although addressed to competent authorities, the aforementioned guidelines provide valuable insight into supervisory practise and are therefore of relevance for institutions as well. Despite their importance for institutions, the draft guidelines at hand do not contain any reference to EBA/GL/2017/05. In order to avoid potential inconsistencies or discrepancies in interpretation between EBA/GL/2017/05 and draft guidelines at hand and as the concrete focus items of both (draft) guidelines vary, we would appreciate clarification on the content related relationship between both (draft) guidelines. Concrete questions on the consideration of requirements of EBA/GL/2017/05 for the implementation of the draft guidelines have been included within Part C below.

C. Specific comments

- Editorial note:

In paragraphs 6 – 8 reference is made to paragraph 8 for defining financial institutions. Instead, reference should be made to paragraph 9. Moreover, numbering of paragraphs should be unique in order to avoid potential uncertainties. As subject matter, scope and definitions are expected to display a mandatory part of the final guidelines, numbering of paragraphs should not re-start with the actual content.

- Definitions:

In addition to the generally accepted three objectives of information and data security, namely confidentiality, integrity and availability, the provided definition of an operational or security incident targets also authenticity and continuity. While we agree with including confidentiality, integrity and availability into the definition, we seek clarification on the dimensions of authenticity and continuity regarding ICT systems and services particularly in contrast to integrity and availability of those.

We would further appreciate insight on the rational for including authenticity and continuity in addition to confidentiality, integrity and availability.

- Paragraph 3:

According to paragraph 3, the management body shall ensure that the budget allocated to fulfilling the requirements related to the institution's ICT governance is appropriate and *sustainable*. We fully support supervisors' expectations on institutions to ensure an appropriate budget for meeting its requirements on ICT governance and also agree to having an *overall* sustainable budget, which is in our understanding to maintain the ability to i) meet its current as well as expected future financial obligations and ii) sustain growth, both primarily through current or past income. Nevertheless, we question the requirement of having a sustainable budget for such a limited scope as ICT governance, particularly as the support of operational needs and implementation of risk management processes is associated with costs and not directly related to income. We therefore suggest deleting the requirement of a sustainable budget for setting an adequate internal governance and control framework. Alternatively, we seek clarification on what is expected to be a sustainable budget within the given scope of ICT governance.

- Paragraphs 7 – 9:

Chapter 4.2.3. outlines, without prejudice to the upcoming EBA Guidelines on outsourcing arrangements, guidelines on the relation to third party providers, including contractual minimum requirements. We are generally of the opinion, that requirements related to outsourcing or other third party procurements should be bundled within one set of requirements, namely the recently published EBA Guidelines on outsourcing arrangements (EBA/GL/2019/02) in order to avoid fragmentation of requirements and inconsistencies across services, activities and functions being outsourced.

- Paragraph 8:

Furthermore, we are of the opinion that the minimum contractual content outlined within paragraph 8 is too extensive for the entirety of potential ICT related services or systems procured from third parties. Rather, the assessment of necessity of specific contractual requirements should be within the responsibility of the institution, whereas, in line with the principle of proportionality, necessity should be assessed risk based. Hence, we suggest, in line with paragraph 7, to limit paragraph 8 to (material) outsourcing of ICT services and ICT systems as otherwise the principle of proportionality and the draft guidelines objective to focus on risk might be contradicted.

- Paragraph 9:

Similarly, we consider the requirement to "seek assurance on the level of compliance of ICT service or system providers with their security objectives, measures and performance targets" as too prescriptive and inexpedient. Monitoring and potential assurance of compliance should be appropriate to the service's or system's relevance and risk it poses, whereas the assessment of associated risks is conducted by means of various mandatory risk assessments as outsourcing risk assessment, vendor risk assessment and information security risk assessments, to name only but a few. The costs associated with a mandatory assurance of compliance of the entirety of ICT service or system providers irrespective of their relevance and risk, is excessive compared to the potentially associated benefits of such mandatory assurance of compliance. We therefore suggest to limit the applicability of paragraph 9 to "where considered appropriate in terms of related risks" i.e. in case of (material) outsourcings.

- Paragraph 13:

Paragraph 13 provides a non-exhaustive list of processes to be implemented as part of the ICT risk management framework, including processes for determining the risk tolerance for ICT risk. We would like to note, that rather than the risk tolerance, the institution's risk management framework contains processes to determine the institution's risk bearing capacity, based on which the institution's management has finally to decide on how much risk it is willing to take. While we agree that comprehensive policies, processes, limits and controls implemented as part of the institution's risk management framework are of utmost importance for determining the maximum risk tolerance (set by the total risk bearing capacity) and are crucial for setting the institution's appropriate risk tolerance, the risk framework as such cannot determine the actual risk tolerance. We therefore suggest to consider rephrasing lit. a of paragraph 13 respectively as follows:

"*a) enable the management to determine an appropriate risk tolerance for ICT risks, […]*"

In order to account for a timely mitigation of risks identified as well as tracking of implementation of mitigating measures, we suggest including an additional item lit. f to paragraph 13 addressing the aforementioned aspects.

- Paragraph 15:

We agree that a mandatory regular review is necessary to consider potential changes adequately occurring throughout the year. Nevertheless, we consider an approval only necessary in case of

changes to the ICT risk management framework, as an approval of an unchanged ICT risk management framework is inexpedient.

- Paragraph 18:

Paragraph 18 requires the institutions in scope to classify business functions, supporting processes and information assets in terms of criticality. The EBA Guidelines on ICT Risk Assessment under the Supervisory Review and Evaluation Process (EBA/GL/2017/05) outline conditions for identifying critical ICT systems and services, whereas no reference to these guidelines is made within the draft guidelines at hand. We ask EBA to provide clarification on the relationship between the requirement of paragraph 18 and the assessment of criticality as outlined in paragraph 41 of EBA/GL/2017/05. Clarification on this point would be of relevance also for further paragraphs, where criticality is mentioned, such as paragraph 49.

Further, we are of the opinion that the costs associated with classification of supporting processes and information assets in addition to the business functions clearly exceed potential benefits. We therefore suggest limiting classification in term of criticality to business functions only and, if considered necessary, to major supporting processes related to critical business functions.

- Paragraph 21:

Following our comment on paragraph 18, we are of the opinion, that carrying out risk assessments, i.e. classification in terms of criticality, on supporting processes and information assets is generally inappropriate and in particular too prescriptive. Consequently, we ask EBA to limit the applicability of paragraph 21 respectively. In case EBA does not follow our reasoning and intends to introduce the classification of supporting processes and information assets in addition to business functions, we would like to express our view, that risk assessments of the aforementioned subjects should rather be reviewed risk based. In line with this, major changes as listed in sentence two of paragraph 21 or changes in the underlying ICT risks and related ICT systems should trigger a re-assessment of risks.

- Paragraphs 23 – 24:

In addition to providing guidance on risk mitigation, we would appreciate clarification of supervisory expectations on risk acceptance (s. comment on paragraph 13), risk avoidance as well as transfer of risks.

- Paragraphs 34 – 40:

We highly appreciate that the guidelines specified on logical security, physical security and ICT operational security follow the content of generally accepted standards as ISO 27001/02 or the NIST Cyber Security Framework, as it contributes considerably to harmonising applicable requirements. However, the EBA draft guidelines at hand deviate particularly with regard to the structure of the aforementioned standards, what exacerbates reading of those. We would highly appreciate further alignment of the guidelines on logical security to the standards mentioned and structure them along security domains or functions to enhance readability.

- Paragraph 63:

Paragraph 63 requires ICT system backups to be stored *sufficiently* remote. While we see the necessity to leave sufficient room for flexibility in interpretation, we would appreciate further specification on supervisory expectations on what is expected to be sufficiently remote through e.g. reference to standards in order to avoid discrepancies in implementation.

- Paragraph 66:

Paragraph 66 particularly emphasises the implementation of the ICT strategy through ICT projects. We would like to note that objectives of the ICT strategy could be implemented by various equivalent means, whereas projects display only one possibility. Irrespective of the means of implementation as well as the concrete strategic objectives, implementation of an institution's strategy should be anytime effectively supported through adequate governance processes. As already outlined as part of our general remarks under B, we consider such requirements as misleading as they might be interpreted by institutions as supervisors expectation to implement ICT related strategic objectives exclusively through projects. Instead of focusing on project setups, clarification of supervisors' expectations should focus on guidelines on an adequate control or change management framework (s. Chapter 4.6.3.).

- Paragraph 84:

As part of sound business continuity management, financial institutions should conduct a business impact analysis (BIA) by means of, among others, scenario analysis. We would like to point out, that according to our understanding, the scope of the BIA is to analyse financial institutions' exposure to severe business disruptions. The impact derived from such disruptions does not change depending on the underlying scenario (root cause triggering the disruption). Consequently, scenario analyses do not provide added value within this context. In contrast to this, scenario analyses can add value in other areas of business continuity management as business continuity planning, response planning and testing. We therefore suggest amending paragraph 84 in such a way that scenario analysis is not expected to be a mandatory part of BIA.

- Paragraph 93:

Financial institutions should test their Business Continuity Planning (BCP), and ensure that the operation of their critical business functions, supporting processes, information assets and their interdependencies (including those provided by third parties) is tested at least annually. While we generally agree that testing of operations is an important aspect of risk management in general and BCP in particular, we are of the opinion, that testing of services provided by third parties should be limited to "where applicable". This follows widely applicable standards on outsourcing and is in line with paragraph 95 lit. a), according to which financial institutions' testing of BCP should include "testing of services provided by third parties, where applicable". We therefore suggest rephrasing of paragraph 93 as follows:

"93. Financial institutions should test their BCPs, and ensure that the operation of their business functions, […] and their interdependencies (including those provided by third parties, *where applicable*) are tested at least annually.[…]."

* * *

We are at your disposal to discuss the issues raised and proposals made if deemed useful.

Faithfully,

Markus Kügel Marija Kožica