Deutsche Bank

EU Transparency Register ID Number 271912611231-56

Deutsche Bank AG
Winchester House
1 Great Winchester Street
London EC2N 2DB

Tel +44 20 75458000
Direct Tel +44 20 75451903

13 March 2019

DB response to the European Banking Authority (EBA) Draft Guidelines on Information and Communication Technology (ICT) and security risk management

Dear Sir or Madam,

Deutsche Bank welcomes the opportunity to provide comments on the Draft Guidelines on ICT and security risk management ("the guidelines").

We support the EBA's objective to ensure sound ICT and security risk management in the EU financial sector and a level playing field for all institutions. In the light of continued evolution of business models and market structure, it will be increasingly important that regulation, including these guidelines, are applied to the full scope of entities involved in the provision of financial services. We are also supportive of the EBA's intention to apply a principles-based approach to informing ICT and security risk management.

There are a number of instances where the draft guidelines depart from that intended approach, with certain requirements being overly prescriptive. This could constrain the ability of large institutions to anticipate and adapt to developing ICT risks. To avoid this outcome, there are a number amendments to the current drafting that should be considered:

I. **Management Board (MB) responsibilities:** whilst it is clearly the responsibility of the MB to ensure that there is an effective framework in place to manage ICT risk, as currently drafted the guidelines risks setting those requirements at too granular a level. This would include requiring the MB to be directly involvement in the design and implementation of a specific risk type (of over 250), without appropriate scope for delegation. The granularity of the responsibilities proposed would go beyond the strategic role of the MB and would be more effectively undertaken by delegation to senior management or governance forum in an overarching risk framework.

II. **ICT risk management framework:** the proposed requirements in section 4.3 of the draft guidelines would apply an overly prescriptive approach to an institution's implementation of the three lines of defence model. This would risk undermining existing, effective enterprise risk management designed to address ICT risks. A principles-based approach,

focused on outcomes, i.e. requirement for an independent risk control and internal audit function for the management of risks, would avoid this risk.

III. **Business continuity management (BCM):** section 4.7 of the draft guidelines risks creating a discrete and additional layer of ICT-specific BCM requirements. This would conflict with an holistic approach to organisation-wide BCM and could constrain emerging approaches to ensuring operational resilience. We recommend the EBA reconsider inclusion of BCM elements in the final guidelines to avoid introducing unnecessary complexity for institutions and a siloed approach to BCM.

Detailed comments on the consultative document are set out in the attached annex. We would be happy to discuss these or any other points with the EBA as it finalises the draft guidelines.

Yours faithfully,

Matt Holmes
Head of Regulatory Policy

Annex 1 - Detailed response

Management Board role and responsibilities

Deutsche Bank is supportive of the overall objective of section 4.2.1. However, we are concerned that as drafted the proposed requirements would significantly expand the management board's (MB) obligations, to include specific responsibility for day-to-day activities regarding the design and implementation of ICT governance and strategy. We do not believe that this level of granularity is appropriate or necessary to ensure the MB discharges its obligation to ensure that an adequate control framework is in place, as per paragraph 2.

In particular, in paragraphs 4 and 15, while we agree that the ICT strategy should be referenced in the MB-approved business strategy, the detailed obligations set out in this draft cover a level of activity which would reasonably be approved and overseen at a level below the MB. We therefore recommend that paragraphs 4 and 15 be amended as follows:

> 4. *The management body has overall* ***accountability*** ~~***responsibility***~~ *for* ***ensuring an effective risk management framework for ICT risks is in place, including ensuring there is an identified individual or forum within the organisation which is responsible*** *for setting, approving and overseeing the implementation* ***of that framework.*** ~~***of financial institutions' ICT strategy as part of their overall business strategy as well as for the establishment of an effective risk management framework for ICT risks.***~~
>
> 15. *The* ***management body should ensure that the*** *ICT risk management framework* ~~***should be***~~ ***is*** *approved and reviewed, at least once a year, by the* ~~***management body***~~ ***individual or forum with delegated responsibility for ICT risks****. Financial institutions should ensure that before any major change of ICT system or ICT services, processes or procedure, and after any significant operational or security incident they identify and assess without undue delay, whether there are any ICT risks resulting from this change or incident.*

Similarly, paragraph 55 requires that ICT operations are managed based on processes and procedures that are 'documented, implemented and approved' by the management body. Whilst the MB should ensure that the ICT risk framework is appropriate, specific implementing processes and procedures should be able to be approved at a delegate level. Furthermore, it is not possible that the MB would 'implement' any policy that it would approve as this extends beyond its strategic role in the governance of the organisation. We therefore recommend that paragraph 55 be amended as follows:

> 55. *Financial institutions should manage their ICT operations based on processes and procedures that are documented, implemented and approved by the* ~~***management body***~~ ***individual or forum with delegated responsibility for ICT risks****. This set of documents should define how financial institutions operate, monitor and control the ICT systems and services, including documenting critical ICT operations and should enable financial institutions to maintain an up-to-date ICT asset inventory.*

4.2 ICT governance and strategy

4.2.3 Use of third party providers

We agree with the objective of this section and the importance of ensuring effective risk mitigating measures when using third parties. It is also important that this section remains consistent with the existing outsourcing and procurement obligations of financial institutions, as set out by the EBA in this section.

Therefore, we recommend that paragraphs 7-9 be amended, to help avoid any overlapping obligations which go beyond the current vendor risk obligations and intragroup service risk controls:

> 7. *Without prejudice to the EBA Guidelines on outsourcing arrangements (EBA GL 2019/**02**) 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 operational functions of payment services and/or ICT services and ICT systems, are outsourced, including, **to the extent applicable**, to group entities, or when using third parties.*
>
> 8. *Financial institutions should ensure that contracts ~~**and service level agreements**~~ with the provider (**third party** outsourcing provider **or** group entity~~**, or third party provider**~~) include the following:*
>
> a) *appropriate and proportionate information security objectives and measures including requirements such as minimum cybersecurity requirements, specifications of financial institutions' data life cycle, and any requirements regarding location of data centres and data encryption requirements network security and security monitoring processes;*
>
> b) *service level agreements, **key performance indicators, reporting or other adequate measures** to ensure continuity of **business-critical** ICT services and ICT systems and performance targets under normal circumstances as well as those provided by **business continuity or** contingency plans in the event of service interruption; and*
>
> c) *operational and security incident handling procedures including escalation and reporting.*
>
> 9. *Financial institutions should monitor and seek assurance on the level of compliance of these providers with their security objectives, measures and performance targets. **For the avoidance of doubt, contractual obligations concerning intra-group service relationships can be satisfied by binding group information security policies applicable to the servicing group entity covering such requirements.***

4.3 ICT risk management framework

4.3.1 Organisation and objectives

The effective management of ICT risks – especially in the current context of innovation and digitisation – requires an institution have sufficient flexibility to adapt to evolving technologies and market structures. It is therefore important that the guidelines remain principles-based, with a focus on outcomes, rather than prescribing specific risk management frameworks which may not be suitable for an institution's specific size or structure, and which may also become obsolete as the financial market landscape and related risks change over time.

This concern is especially acute in section 4.3.1, where the guidelines mandate the use of the three lines of defence (3LoD) model for the identification and management of ICT risks. This poses a number of issues.

First, this prescriptive requirement extends beyond the current body of regulation which instead requires an independent risk control and internal audit function for the management of all risks. The management of ICT risks is important to protect both the institution and its customers, however, ICT governance should be embedded in an institution's established (and approved) risk governance framework, and should not require the establishment of a distinct risk management framework just for ICT.

Second, there is no consistent industry standard for the 3LoD model. Various institutions interpret and implement the 3LoD model based on their respective size, structure and complexity, and have differing views on the most effective allocation of responsibilities and accountability. For example, the allocation of information security roles to first or second line is not consistent in the industry, however, this does not necessarily result in an inferior model or outcome for the management of ICT risks. Furthermore, current national regulation for ICT risk (including the BaFin BAIT circular in Germany) indicates the need for a separate and independent function or division to oversee this risk, without a further split into first and second lines of defence.

Applying a standardised approach to the 3LoD model, on the other hand, would risk disrupting the existing, effective enterprise risk management practices of large institutions which already achieve the guidelines' intended objectives for ICT risks.

We do not believe this was the intention of the EBA, but rather to provide guidance for smaller or less mature institutions on how to achieve appropriate separation of certain functions, such as the information security function from the ICT operations processes. As mentioned in the hearing from 13 February 2019, we would welcome clarification by the EBA that the guidelines do not aim to force well-established institutions to alter current practices which meet the existing regulations and effectively manage ICT risks.

We fully agree that the segregation of duties and the establishment of independent controls functions are essential for an effective internal controls system. However, the EBA's regulatory objectives would be better achieved by setting out principle expectations, and using language consistent with its other guidelines and directives (e.g. EBA Guidelines on Internal Governance under Directive 2013/36/EU (CRD IV) and Article 74 of CRD IV), while leaving the specific organisation and divisional implementation at the discretion of each financial institution.

We therefore recommend the EBA avoids specifically detailing how the 3LoD model should be implemented for ICT risks and amends paragraph 10 to highlight the intended outcome:

> *Financial institutions should identify and manage their ICT risks according to* ~~*the three lines of defence model*~~ ***an effective internal risk management and control model, including an independent risk control function, to identify and manage these risks****. PSPs other than credit institutions may use an equivalent internal risk management and control model, to identify and manage these risks. Financial institutions should ensure that their internal control function has sufficient authority, independence, resources, expertise and direct reporting lines to the management body.*

The 3LoD model in paragraph 11 may however still prove useful for certain institutions with less mature risk management functions. The EBA should instead move this to the Annex as an example of a potential model framework. This would provide the broad scope of entities covered under the guidelines with additional insight without unduly constraining or introducing complexity for large institutions and their enterprise risk management. However, we recommend that the wording for this example be updated as follows:

> *Where the three lines of defence model is applied, the ICT function(s) in charge of ICT systems, processes and security operations, acting as the first line of defence, should operate under the* ~~*supervision*~~ ***oversight*** *of an internal control function acting as a second line of defence. This internal control function should* ~~*take responsibility for the*~~ ***independently challenge the first line of defence's*** *management of ICT risks. The internal audit function, acting as the third line of defence should have the capacity to independently review and provide assurance of the respective roles the first and second lines of defence (see section 4.3.6).*

4.3.3 Classification and risk assessment

While we agree that an annual assessment of critical processes is reasonable, requiring such as assessment at an even shorter interval would be disproportionate and should not be mandated.

Generally, periodic risk assessments should not be required for all sourcing arrangements and should instead rely on a risk-based approach depending on the subject's criticality. Periodic assessment should focus on where an institution has (i) risk or (ii) major changes, to either the risk situation of the institution, the internal or third party control environment or the nature of the outsourcing arrangement.

4.3.5 Reporting

As noted in our response to 4.3.1, the management of ICT risks should not be treated differently than other risk types within a broader enterprise risk management. ICT risks are part of an integrated report to the MB, and if they are indeed deemed as a top risk for the institution it will be specifically mentioned.

The MB should have the ability to delegate to an individual or forum, if deemed appropriate, to ensure its time is not dedicated to reading individual risk reports which are not critical for the MB to review. We therefore recommend paragraph 25 be amended as follows:

Risk assessment results should be reported to the ~~*management body*~~ ***individual or forum with the delegated responsibility for ICT risks*** *in a timely manner. Additionally, PSPs should provide competent authorities with an updated and comprehensive risk assessment as laid down in Article 95(2) of Directive (EU) 2015/2366.*

4.4 Information security

4.4.2 Information security function

As noted in our response to section 4.3.1, prescribing a specific risk framework – in this case the 3LoD model – should be avoided and instead the guidelines should highlight the intended outcome.

The focus for this requirement should be on the required level of independence of the information security function and not the organisational structure of the financial institution. The guidelines could further elaborate on requirements to demonstrate this function's independence to ensure a more consistent view across institutions whilst permitting the needed organisational flexibility.

This criteria could include, for example: appropriate segregation from ICT operations processes; and the designated person responsible for information security to report directly to the MB.

4.5 ICT Operations management

In regard to paragraph 56, while we agree with the potential benefits that the automation of ICT operations may provide, this is not without its own risks or the sole method of achieving additional operational efficiencies. We recommend the EBA retain its intended principles-based approach and either remove paragraph 56 or amend it as follows:

To increase the efficiency of financial institutions' ICT operations, financial institutions should~~*, as far as possible, automate ICT operations (e.g. job scheduling processes, monitoring of ICT systems, maintenance and repair of financial institutions' assets, shift handover) to minimise potential errors arising from the execution of manual tasks. Financial institutions should ensure that the performance of their ICT operations is aligned with the business requirements*~~ ***consider where automation of ICT operations may provide material benefit in the minimisation of potential errors arising from the execution of manual tasks.***

4.7 Business continuity management

It is unclear why business continuity management (BCM) is presented in the guidelines as a subset of ICT risk. This section of the guidelines varies from providing very specific guidance for ICT functions to more strategic requirements on an institution's overall BCM.

BCM is a core component of an institution's Operational Resilience. Emerging approaches to (and potential supervision of) this topic focus on ensuring the availability of business services end-to-end in the event of operational disruption and irrespective of the cause. The associated

tolerances for disruption will be defined top-down and across a suite of severe but plausible scenarios. While they may be current/topical, not all of these scenarios will be IT-related.

This focus on service availability, and appropriate senior management accountability, is a sensible evolution because it enables prioritisation and more holistic evaluation of capabilities. By setting specific requirements for one function (i.e. ICT), at the expense of all other functions, the guidelines would undermine this emerging approach. They would create a discrete and additional layer of BCM requirements specifically for ICT, as opposed to the business as a whole.

The resilience approach for the business as a whole covers the ICT functions and it is therefore important to ensure this remains consist across the board as part of organisation-wide BCM. Otherwise, this may lead to ambiguity in policy design and implementation, unnecessary complexity in terms of control standards, and potentially reinforce siloes by enabling a higher level of assurance for ICT than the client-facing functions they support.

While we fully appreciate recent concerns around disruption caused by technology failures, poor change management or inadequate cybersecurity, the guidance applies a narrow lens to BCM which may deflect focus from other, and equally important, impact types. A narrow lens may be useful where institutions have a relatively contained number of centrally-maintained business continuity plans, as implied in sections of the guidance, however, effective assurance for large global banks relies on an approach that can be consistently applied across all business divisions and jurisdictions.

We therefore recommend the EBA reconsider the inclusion of the BCM elements outlined in this section to avoid introducing unnecessary complexity to institutions and a potentially siloed approach to BCM.

4.8 Payment service user (PSU) relationship

We welcome the guidance set out in this section regarding the activities of payment service providers (PSPs), however, certain requirements would benefit from additional specification to help avoid confusion as to which category of participant must implement them.

For example, while the term 'PSP' is used throughout the guidelines we believe certain requirements in this section are only applicable to either a credit institution or a Third Party Payment Service Provider (TPP). The guidelines should therefore specify when a requirement applies to all types of PSPs and when they are directed specifically at an Account Servicing Payment Service Provider (ASPSP), Payment Initiation Service Provider (PISP), and / or Account Information Service Provider (AISP).

In particular, we recommend that the EBA clarifies that paragraphs 101-103 should only apply to ASPSPs. Establishing or disabling specific payment functionalities should be initiated and processed only by these entities as this is the level at which the decision is made, i.e. Directive 2015/2366/EU (PSD2) does not allow for establishing or disabling specific payment functionalities through a TPP.

Another consideration relates to the need to make the relationship between the TPPs and the ASPSPs transparent for PSUs. We believe that the PSU should always be made aware by TPPs that they are not acting on behalf of the ASPSP. This will help ensure stronger consumer

protection as it will allow PSUs to make more informed decisions and maintain consumers' trust in the developing payments system.

In order to prevent the trust that the PSUs have in the ASPSPs from being misused, we suggest that section 4.8 require the TPPs to clearly articulate to the PSUs whether or not it is acting on behalf of the ASPSP. To make such statement obvious to the PSU, it could be provided in a disclaimer when an instruction is initiated or added to the TPP's documentation or guidance for the PSU.