22 December 2016

EBF_024231E

EBF Response to EBA Consultation on Guidelines on ICT Risk Assessment under the SREP (EBA-CP-2016-14)

Key points:

- The guidelines are presented in a coherent way and are compatible with the SREP process and current practices in banks.
- The guidelines and their application should be further governed by the principles of flexibility and proportionality.
- It is unclear how the principle of proportionality will be applied across different jurisdictions and to global institutions. Clarification would insofar benefit the banks and their regulators. Proportionality must guide regulation and its implementation.
- There is a number of regulations and initiatives that address ICT risk. Overlap and inconsistent requirements should be avoided.
- The level of involvement of the Management Body should be coherent with the internal governance framework of each bank. It should be explicitly acknowledged that the Management Body can internally delegate the execution of the principles, functions and expertise relating to ICT risk.
- We understand that ICT risk is part of operational risk, but it should be assessed in further detail. Therefore, a coherent approach to operational and ICT risk is needed.
- Finally, banks should remain free to manage risks using their own taxonomies.

General Remarks

In general the contents of the guidelines are presented in a coherent way and are compatible with the SREP process (focus on governance, escalation processes, risk taxonomy and control processes). To a large extent we find that the guidelines cover processes and controls that are already in place in the current approach.

Duplication and Proportionality:

However, there is concern among the EBF's Members that there are a number of regulations and initiatives currently in place or being developed which address similar issues of ICT risk and therefore that there is a danger of **overlapping and inconsistent requirements** being placed upon institutions in scope of the Guidelines. For example, the ECB has recently completed a thematic review on cyber risk, a risk that currently falls under the wider umbrella of ICT risk. This is also true at the international level with various initiatives from MAS, Swiss and Irish authorities for example. Members would welcome a call for harmonisation of approaches across jurisdictions and would welcome the EBA's leadership in this regard, especially around topics like cyber which is often a cross-jurisdictional problem.

Moreover, we would like to know if there is more precise guidance on the processes to be considered as relevant at the international level within the scope of the Guidelines. There is a concern among members as to the applicability of **the principle of proportionality** across different jurisdictions and when applied to global institutions. Currently there are several provisions around proportionality which are not consistent and would duplicate work. The Guidelines would benefit from clarification as to how proportionality was being judged, especially in the case of global banks. Will proportionality be assessed in the context of the market?

European Banking Federation aisbl

Brussels / Avenue des Arts 56, 1000 Brussels, Belgium / +32 2 508 3711 / info@ebf.eu
Frankfurt / Weißfrauenstraße 12-16, 60311 Frankfurt, Germany
EU Transparency Register / ID number: 4722660838-23

Finally, it is not clear how the Guidelines will be incorporated in the SREP assessment. One of the main points of concern here is whether banks need to have a specific assessment on ICT risk. Our understanding is that ICT Risk is **part of Operational Risk**, but the ICT Risk Assessment could be performed with a deeper assessment that complement the OR Assessment. How will the ICT risk assessment be factored into the evaluation of Operational Risk for ICAAP purposes? Will it contribute to the "Expert Judgement"?

The Management Body:
Activities included in the proposed guidelines would be too demanding if imposed directly and solely on the management body (the Board of Directors). It would require a considerable time to convey and implement and could potentially affect the ability of the Board to cover and deal with other equally important matters. The role of the Board of Directors as the Management Body should not encompass the wide range of activities, principles, functions and expertise that the document outlines. Instead we think that the level of involvement of the Management Body should be coherent with the internal governance framework of each bank and, therefore, not all the tasks and activities identified and assigned in the guide to the management body should be directly addressed, at least with this granularity, by the Board of Directors.

We propose that the guidelines should explicitly acknowledge that the Management Body can internally delegate the execution of a large part of the principles, functions and expertise relating to ICT risk included in the proposed guidelines with the Board retaining the top management and supervisory function.

Use of "ICT Outsourcing Risk":
The wording of this ICT Risk Category suggests processes that are contracted out of the organisation. Since the definition of the term includes 'engaging a third party' we suggest that the Risk Category is re-named "ICT Supplier Risk" to provide a broader coverage than only outsourcing.
Example: 3 Background and rationale: §2: Definitions

Risk Taxonomy:
While the Risk Taxonomy is designed to unify the Europe-wide review of ICT risks, we would wish to see that **banks retain latitude to manage risks using their own taxonomies**. We welcome statements made at the public hearing on the Guidelines which took place 22 November in London, which reinforced this latitude. The statements made were to the effect that firms would be free to use frameworks that they consider appropriate for managing ICT risk and the EBA does not consider its objective is to develop a formula or methodology for risk tolerance/thresholds owing to the difficulty in measuring operational and ICT risk. These are important points as mandating any taxonomy in the management of risks within firms might remove the opportunity for the management of risk in a way that matches the enterprise-wide approach. Such a move could present a further danger that categories are seen as complete thereby constraining a firm's thinking around its risks. Also, the notion or taxonomy should be clarified, in order to correctly allocate the incidents under the proper ICT risk categories.

Industry-wide Suppliers and Schemes:
As the EBA has acknowledged, it is difficult to measure operational and ICT risk. As discussed below, this is in large part due to the cross-jurisdictional nature of ICT functions especially in global institutions. Members believe that a better co-ordinated approach to industry-wide suppliers might reduce the expected burden on regulatory bodies and firms. While providers of credit referencing, national telecoms providers, ATM and payment transmission networks can be considered as a repeated supplier to multiple firms, we would prefer that these common, industry-wide suppliers were considered on an industry basis rather than having multiple points of view of the same supplier. This might include supplier resilience, security, governance and risk management. It is the case that individual firms cannot necessarily assess industry concentration risk associated with these 'critical' suppliers.

Maturity levels, scoring or KPIs

We also recommend that the guidelines include more details about how to get to the maturity levels, scoring or KPIs. The draft guidelines use COBITv5 as a basis. That version has specifically been put together to measure the maturity of implementation of the controls defined in the framework and describes

all the necessary ingredients for the determination of every maturity level. So we would advise to further use these elements of the COBITv5.

Continuous or agile delivery
We also would like to emphasis strongly on what was stated on section 3.3.4 – that it needs to provide also for the adoption of continuous or agile delivery.

Detailed comments

In the following section, we shortly summarise the points in which we see further need for clarification and or more level of detail:

2. Subject matter, scope and definitions

EBF Members would welcome more precision. On page 11 section Definitions, there are some basic definitions of terms. These definitions are not fully-aligned with NIS directive definitions. We think that it is important to provide a consistent language that has definitions that are aligned to avoid overlaps and confusion.

- Example from the NIS directive, article 4: Definitions:
  - (2) 'security of network and information systems' means the ability of network and information systems to resist, at a given level of confidence, any action that compromises the availability, authenticity, integrity or confidentiality of stored or transmitted or processed data or the related services offered by, or accessible via, those network and information systems;
  - (9) 'risk' means any reasonably identifiable circumstance or event having a potential adverse effect on the security of network and information systems;
- ICT Risk Assessment – Definitions
  - "ICT security risk: The risk of unauthorized access to ICT systems from within or outside the institution (e.g. cyber-attacks), as further elaborated in the Annex."

It would be good to have common definitions for all EU documentation. Currently, there are ad-hoc definitions in the NIS directive, in this specific paper, and even in the SSM Cyber Incident Pilot.

Additionally, the definitions proposed are not very consistent internally with the annex "ICT security risk: The risk of unauthorized access to ICT systems from within or outside the institution (e.g. cyber-attacks), as further elaborated in the Annex.": Some of the details included on the Annex have nothing to do with "unauthorized access". For instance, for Distributed Denial of Service attacks (DDoS), which is one of the examples included in the annex, there is no kind of "unauthorized access" to your systems.

Many institutions use the term "ICT services" in different forms, but never in the way as defined herein. Since in the following sections this definition is referred to, in particular when determining critical IT, we propose a clearer and more comprehensible definition of what "ICT services" refer to. We would rather classify this definition more by the term "business-process with ICT-relevance", because almost all ICT systems are used to support business processes of an institute.

The proposed ICT Risk Taxonomy formed by the 5 definitions under paragraph 9 is focused on risk drivers that are not complementary to each other. This can lead to an overlap by causing some undesirable issues of attribution of the risk.

For instance, in case of an event of a "not authorized change" that leads to data corruption, it would be difficult for banks to assess which risk is predominant between "ICT change risk" or an "ICT integrity risk". Similarly, if an incident is generated by an "unauthorized access" to the systems and leads to a system-down, it is difficult to categorize such incident as an "ICT security risk" rather than an "ICT availability and continuity risk".

Considering the above, we would ask for a clarification on how the taxonomy should be interpreted, in order to correctly allocate the incidents under the proper ICT risk categories given in the guidelines.

Regarding the "ICT Outsourcing risk category", we would suggest to separate the ICT consequences arising by the activities provided by the outsourcee (that should be linked to the other 4 ICT risks on pages 11-12) from the risks derived from the choice and management of the aforementioned outsourcee (service provider).

In addition to the proposal to have common definitions for all EU documentation, EBF members would like to suggest to consider an even broader synchronisation of definitions. As a lot of European banks have a global presence and make use of international ICT service providers, definitions of international standards (e.g. ISO 27000, ISO 22300, ISO 29100) should be taken into account.

Title 2 - Assessment of institutions' governance and strategy on ICT

2.2: ICT strategy

Members disagree with the inclusion of the need to 'keep ICT up-to-date' and the treatment of important and complex ICT changes in paragraph 23. It is the view of the industry that while strategy should set a framework for long-term management of the ICT estate and approach to change, details on these specific items might be more usefully covered in other sections.

2.2.1: ICT strategy development and adequacy:

Throughout Title 2 EBF Members are concerned about the definition and required role of the Management Body. This holds true across all recent EBA/ECB consultation.

The definition of the Management Body should be coherent with the definition used in internal governance, including relevant committees and delegation of duties. Further, paragraph 26b should be amended to include a materiality element. The EBF's Members do not consider that the Management Body must know and address all risks associated with ICT – but should know and address *material* risks associated with ICT.

There is a mention of the IT function being "sufficiently staffed," however it is not clear how this will be assessed. We think that the operating model of each bank has to be assessed on a case-by-case basis and, for example, different levels of outsourcing have to be taken into consideration. If the idea would be to compare the level of staffing to a common benchmark across the industry this could potentially be misleading. As a corollary to this point, we propose that a strategic approach to suppliers might be included in paragraph 24.

Title 3 - Assessment of institutions' ICT risks exposures and controls: Reference to "paragraph 127 of Title 6 of the EBA SREP guidelines" under paragraph 35

Paragraph 127 of Title 6 of the EBA SREP guidelines points to "peer-benchmarking". Operational risk is very different from institution to institution (e.g. process-oriented, varying IT systems) and the measurement methods of OpRisk also differ from institution to institution. Therefore, benchmarking is from our point of view not a meaningful approach.

The paper does not spell out that there could be potential compensating controls to mitigate risks as a result of some controls not being in place. Most controls are described on a standalone basis, not considering the controls mix that can be sufficient also (not all controls need to be addressed to still have a controlled environment if we take a more holistic view).

53b - ISO 27015 ISMS for Financial Institutions is withdrawn by ISO JTC1- SC27 in October 2016 and should therefore be removed as reference.

3.2.1: Review of the institution's ICT risk profile: Relevant information about "institution's risk exposure" under paragraph 37

For EBF Members it is not clear whether these are really the main risk drivers for an institution. In the "S.W.I.F.T" incident as an example, they were no complex institutions, they had no internet-business and are not outsourced, but the risk was tremendous. Therefore, we suppose a stronger orientation of the referenced risks to the criticality of the respective business processes and underlying IT systems for this purpose.

Section 3.2.2: Review of the critical ICT systems and services (paragraph 38)

How do you define this as it is not what is viewed as "critical"? It could potentially be very costly both for the supervisor and for banks to assess the controls of risk on all systems and platforms.

Paragraph 38 states that competent authorities should review documentation from institutions in order to identify ICT risks with a potential significant prudential impact. As stated above, the international character of many of the institutions in the scope of these guidelines and the cross jurisdictional nature of ICT risk creates a complicated risk profile for regulators to judge. As a result, institutions are facing multiple regulatory jurisdictions requesting increasing amounts of increasingly granular data. Authorities would thus benefit and should seek to develop an engagement framework that creates the least amount of duplication across different regulatory jurisdictions.

Section 3.2.2: Methodology to identify critical ICT systems and services under paragraph 39 and/or 50

Although the considerations under paragraph 39 are broadly appropriate, the requirement that services should 'fulfil at least one of the following conditions' might scope in too many services to the list of 'critical' items. The EBA should consider whether it would be preferential for firms to be obliged to rate or tier critical services – allowing each firm to define their own criticality approach and affording a more nuanced approach than 'critical' or 'non-critical'. This list might then serve as a non-exhaustive list of considerations in this tiering or rating.

It is also the case that the criticality of ICT systems and services of an institution are not primarily structured along a one-dimensional perspective, but rather along organizational and process-related multi-dimensional criteria. This depends usually on the institution's risk-framework and one reason for this is the Segregation of duties. Therefore an alternative approach could be a more process-oriented methodology to identifying critical ICT systems, ICT services and critical baseline functionalities under consideration of the institution's organizational structure. These methodologies do not exclude criteria such as Recovery Time Objectives (RTO) or storing sensitive data from being considered.

Clarification is also sought about the inclusion of the risk of "confidentiality" in the "ICT security risk", as a criteria for what is critical. Including this as a trigger may extend the scope to almost everything

Further, external system risk IT components should be addressed in the Guidelines.

Finally, although Members agreed with the conditions given for identifying critical ICT systems and services and were confident in their ability to comply, there is concern over the process of complying especially for cross-jurisdictional banks. The potential workload for demonstration of appropriate consideration of risk could be onerous and therefore the industry urges the EBA and competent authorities to engage in dialogue around how duplication can be minimised and workload can be minimised both for authorities and institutions in scope of the Guidelines.

Section 3.2.3: Identification of material ICT risks to critical ICT Systems and Services

It is important to maintain the principle of flexibility in regards to managing ICT risk as such risks are not black and white in nature. The industry is open to a dialogue with authorities as to how to pull together best practice for such a review.

The principle of flexibility is also essential in the assessment of controls to mitigate ICT risk. A high level approach allows institutions to align their internal controls to the given categories reducing burdensome

work for both the institutions and authorities and resulting in a better outcome for managing risk. Further, should too specific an approach be adopted, it could result in a tick-the-box rather than a risk-based approach to compliance by institutions trying to adhere to the guidelines. There is, among banks, a substantial concern over the process of complying, particularly for cross-jurisdictional banks.

Finally, many Members take a customer impact first focus in determining system criticality. While this is mentioned in 40b, we feel that more prominence should be given to this consideration in the form of a distinct bullet point.

Section 3.3.1: ICT risk management policy, processes and tolerance thresholds.

Efficiencies in the application of the guide can be driven here by referencing an already-reviewed enterprise-wide approach to Operational Risk. We suggest acknowledgement is given to a wider Operational Risk approach that regulatory bodies consider to be adequate, rather than re-reviewing this as a distinct ICT Risk management approach.

Section 3.3.2: Organisational management and oversight framework: Paragraph 48e

This item should be refined to make clear whether 'applicable ICT regulations and policies' includes technology-related policies like the adoption of particular technology platforms. We suggest this be refined to say 'risk-material ICT regulations and policies'.

Section 3.3.4: ICT risk controls that are specific for the identified material ICT risks (Para 52.a.i): Dependency Analysis

The need for a 'comprehensive analysis of dependencies between the critical business processes' suggests that a dynamically updated CMDB is mandated by the proposal. We suggest that this is better expressed as 'a mapping between critical business processes and supporting systems'.

Section 3.3.4: ICT risk controls that are specific for the identified material ICT risks (Para 52.b): Data Centre Separation

While we agree that distance between data centres is an important consideration, it should not be the sole consideration and we would suggest the words '…sufficient separation between…' are used. This term might encompass separation geographically, but also by power supplier and telecoms provider.

Section 3.3.4: ICT risk controls that are specific for the identified material ICT risks (Para 52.b.iii): Monitoring

The need to detect ICT availability or continuity incidents should be subject to system criticality and other risk considerations. The wording of this bullet suggests that it might be mandated on all elements of ICT solutions across the firm.

Section 3.3.4: ICT risk controls that are specific for the identified material ICT risks (Para 52.b.ix): DDOS Attacks

This bullet is too tightly-specified to include only DDOS attacks and there is a level of duplication with point v. We would suggest that a wider view of cyber threats is adopted.

Section 3.3.4: ICT risk controls that are specific for the identified material ICT risks (Para 52.c): Continuity

We believe this section should be driven by expected and proven recoverability rather than the need for back-ups. Firms might wish to have multiple copies of data in online redundant stores, but referring to backups only here does not reflect current thinking on ICT resilience.

Section 3.3.4: Vulnerability assessment under paragraphs 53.a.iii

From our understanding the results of a vulnerability assessment are part of the daily operational business. Known vulnerabilities are fed into incident and patch management processes in order to ensure a quick

resolution for the identified vulnerability. Only when the vulnerability(ies) cannot be remedied does a further processing/assessment through the obligatory risk management processes become necessary.

Section 3.3.4: ICT risk controls that are specific for the identified material ICT risks (Para 54): Controls for managing material ICT change risks

Section (b) does not provide for firms to adopt continuous or agile delivery where functions of developer and operator might be combined to a degree but within more highly controlled tools and back-out approaches. Section (c) should better reflect the criticality of a system for replication in a test environment and the wider role of quickly deploying and backing-out changes rather than undergoing extensive proving in non-production environments (the introduction of potentially bad and untested code should be avoided). Section (g) should consider both the risk of the change as defined by the firm but also that security vulnerabilities can be exploited in non-Internet facing software.

Section 3.3.4: Data integrity risks under paragraphs 55 and 56

The requirements set out especially in section 55 a. and 55 b. widen the scope of several BCBS 239 requirements far beyond risk data and the usual procedures in the institutions. We therefore recommend a more risk-based approach.

Paragraph 56 mentions the link to RDA, but we found very little guidance on how these risks will be assessed. We recommend the EBA provide further illustrations of the envisioned assessment criteria.

Section 3.3.4: controls for managing material ICT outsourcing risks

Regarding paragraph 58 " …. and in particular, controls and a control environment in place for mitigating material outsourced ICT services that are commensurate with the size, activities and the ICT risk profile of the institution …".
In our view, the phrase "mitigating material outsourced ICT services" should relate to the outsourced ICT "risks" rather than "services". Hence, for the sake of clarity, we ask the EBA to confirm if such interpretation is correct.

Section 3.4 Risk scoring under paragraph 60

From our point of view, a scoring of risk based on the number of potential risks might be misleading and potentially even incentivise an inappropriate risk exposure unless the actual loss potential is properly taken into account (e.g. under the current model one risk with a potential loss of 5 billion would lead to a better risk score than four equally probable potential risks with a possible loss of 100 million each). Therefore we suggest a change to the considerations for assigning an ICT risk to an approach taking into account a combination of the loss potential and the probability of occurrence.

Annex: ICT Risk Taxonomy: ICT Availability and Continuity Risks

This section does not appear to give adequate prominence to the design and operation of resilient systems. While disaster recovery is one element of availability and continuity we would suggest that a wider view needs to be taken to include automatic resilience, reduction in manual process, monitoring etc.

Annex: ICT Risk Taxonomy: ICT Security Risks

While this section is currently adequate it brings a wider question about how this section can be kept up-to-date and respond to emerging threats and approaches.

About EBF

The European Banking Federation is the voice of the European banking sector, uniting 32 national banking associations in Europe that together represent some 4,500 banks - large and small, wholesale and retail, local and international - employing about 2.5 million people. EBF members represent banks that make available loans to the European economy in excess of €20 trillion and that securely handle more than 300 million payment transactions per day. Launched in 1960, the EBF is committed to creating a single market for financial services in the European Union and to supporting policies that foster economic growth.

www.ebf.eu @EBFeu

For more information contact:

Timothy Buenker
Senior Policy Advisor
Banking Supervision
t.buenker@ebf.eu
+32 2 508 37 22
+32 496 50 12 56

www.ebf.eu