FÉDÉRATION
BANCAIRE
FRANÇAISE

2017.01.06

FBF RESPONSE TO EBA CONSULTATION PAPER ON ICT RISK UNDER SREP (EBA/CP/2016/14)

The French Banking Federation (FBF) represents the interests of the banking industry in France. Its membership is composed of credit institutions authorized as banks and doing business in France, i.e. more than 370 commercial, cooperative and mutual banks. FBF member banks have more than 37,500 permanent branches in France. They employ 370,000 people in France and around the world, and service 48 million customers.

The FBF welcomes the opportunity to comment on the EBA's Consultation on ICT risk under SREP. Please find our main comments below.

General comments

The purpose of defining a common framework for assessing ICT risk is actually needed and we found very relevant and useful the guidance provided by Title 3, especially on the control items to assess.

We fully support the EBA's stance considering ICT risks as part of operational risk and find it very beneficial for ICAAP purposes. We need to have a homogenous approach to ICT risks across institutions, tentatively not only at European level, limiting as much as possible individual discretions. We consider all the consequences of this position should be fully drawn and that the overall framework should be better aligned on the sound principles of operational risk management and the ones currently developed by ICT specialists.

- the European framework would benefit to be as aligned as much as possible with other international standards, in order to avoid national discretion, to create some kind of uneven playing fields and to uselessly complexify ICT risk management within institutions with assessments and reporting to be performed along different standards. More specifically the proposed setup should rely more closely on works such as COBIT, ITIL or NIST referential.
- the framework should also leverage on best practices in operational risk management such as:
  - clear definitions that do not overlap each other
  - causes, event consequences analytical approach
  - alignment with the Basel framework that drives the Internal capital assessment, such as event types that are exclusive from each other
  - Link with IT operational processes(COBIT/ITIL,ISO, …)

  - leveraging on the well-established practices for risk management and governance, which already define the role of the executive and supervisory bodies or the three lines of defence model.

The FBF considers the actual version of the proposed guidelines does not comply with these sound principles and should be amended therefore.

Detailed comments on the draft guidelines

In general, we welcome these draft guidelines. Process and evaluation points are consistent with the SREP. Nevertheless, some issues have drawn our attention, namely:

Definitions proposed in these guidelines:

The definitions given in §2 rise several issues or comments, many of them being also linked to the taxonomy approach suggested in annex (see below):

- as a general comment, risks should be defined by events, ICT failure as a cause should be identified. A reporting on ICT should be a mix of ICT events and events with an ICT cause.
- for a more comprehensive and holistic view, we think ICT should be defined in this document, even if this is already the case in the SREP guidelines. This last definition would benefit from being refined and updated.
- ICT data should be defined (we propose "data stored or processed by ICT systems") and it should be made explicit all mentions of data only refers to ICT data. ICT assets should also be defined.
- ICT security risk could not be limited to the risk of unauthorized access to ICT system but should also encompass the risk from unlawful or unsolicited access to ICT system, such as denial of services.
- ICT Change should be defined through failure in the project management process and named as such. The current definition opens the way for including under this category, failures in the process of implementing change in the production environment that is more a cause of unavailability or integrity or security risks on ICT assets. Furthermore, ICT change risk is defined as the risk coming from the inability to manage change in a controlled and timely manner. The timely manner is arguable (see comment on the taxonomy hereunder and the way obsolescence is accounted for twice in the proposed nomenclature).
- ICT outsourcing is not a risk per se. Outsourcing should be defined as the risk linked to the choice of the outsourcer and its potential default and is not limited to ICT but can also apply to business processes. Apart from this risk view, outsourcing should be considered as a specific risk driver for the other ICT risk category

The ambiguities in the definitions will inevitably rise discrepancies among institutions and even supervisors when using them and trying to assess the associated risks and risks mitigation framework, and eventually the capital requirement.

Annex on ICT risk taxonomy (and § 42):

Taxonomy elements correspond mainly to ICT processes more than risks.
It provides a referential that mixes up causes, event and consequences with significant overlaps in categories and no link with Basel event types. This creates a very critical issue when coming to reportings and assessing capital requirements:

- a same event can be reported and assessed twice and sometimes three or four times
- solving this issue is left at each one discretion, impeding from any consistent view at supervisory level, and probably also at large institution one,
- furthermore, in the ICAAP process, some of these ICT risks which overlaps between themselves, may also be reported in other Basel event type such as internal or external fraud (for instance cyberattacks often materialize through fraud events)

Risks categories should be seek to be mutually exclusive in order to ensure a coherent approach in reporting and assessments. Key categories could be ICT unavailability, ICT security, ICT data integrity and ICT project failure.
These categories may be complemented for analytical purposes by

- Causes such as unintended/ intended failure or damage of a hardware or software, unsolicited control of an ICT system…
- Or risk drivers such as internal driver, third party provider driver, customer driver, other third party driver….

Hereafter are some illustrations of the inefficiencies of the current nomenclature

- inadequate capacity management is more a cause than a risk. The risk is inadequate sizing of ICT systems
- Loss of availability of hardware or software should be seen as a risk more than ICT system failure which is too global
- obsolescence is mentioned in the software unavailability case when it may also affect hardware. Furthermore it is also reported when dealing with the ICT risk linked to inadequate lifecycle and patch management (ICT change risk).
- the "disruptive and destructive cyberattacks risk" seems actually mainly targeting DDOS that is an unsolicited overloading of ICT system
- the "cyberattacks and other external ICT based attacks" seems actually to mainly target unlawful control of ICT system. Risk drivers such as attacks coming from within the institution or a third party provider or …., would be beneficially introduced. Furthermore social engineering cannot be qualified as an attack performed from internet or outside networks. It should be set aside of ICT risks, most of the attempts having no link with the ICT system.
- Inadequate physical ICT security is a cause more than a risk in itself.
- ICT change risks are more causes than would result in loss of availability, security or integrity. The risk linked to the non-delivery of an ICT system in a timely and cost controlled manner does seem to appear properly.
- ICT data integrity risk category targets unintended situation when intended situations are captured through the ICT security risk. This would need to be clarified. Most of the risks

proposed are causes more than risks. Furthermore the data change risk overlaps with the ICT change category.

- Most of the ICT outsourcing risk overlaps with the other risk categories as they may be a driver for unavailability, security or integrity issue.

.