EUROPEAN FINANCIAL CONGRESS

Instytut Badań
nad Gospodarką Rynkową
Do Studzienki Str. 63
80-227 Gdańsk, Poland

tel. +48 58 524 49 01
fax. +48 58 524 49 09

efc@ibngr.pl
www.efcongress.com

Position of the European Financial Congress[1] in relation to the European Banking Authority's consultation paper on ICT and security risk management[2]

Methodology for preparing the answers

The answers were prepared in the following stages:

Stage 1

A group of experts from the Polish financial and IT sectors were invited to participate in the survey. They received the EBA's consultation paper and the consultation questions prepared by the survey project coordinators from the European Financial Congress. The experts were guaranteed anonymity.

Stage 2

The European Financial Congress received responses from individual experts and experts representing:

- banks,
- FinTechs, IT firms and financial infrastructure companies
- regulatory bodies,
- consulting firms and law firms,
- the academia.

All the responses were collected, anonymised and presented to the experts who took part in the consultation. The experts were asked to mark in the other consultation participants' opinions the passages that should be included in the final position as well as the passages they did not agree with. Experts could also adjust their own positions under the influence of arguments presented by other experts.

Stage 3

The survey project coordinators from the European Financial Congress prepared a draft synthesis of opinions submitted by the experts. The draft synthesis was sent to the experts participating in the survey with the request to mark the passages that should be modified in the final position and to propose modifications and additions as well as marking the passages they did not agree with.

Stage 4

On the basis of the responses received, the final version of the European Financial Congress' answers was prepared.

---

[1] European Financial Congress (EFC – www.efcongress.com). The purpose of the EFC is to promote debate on how to ensure the financial security and sustainable development of the European Union and Poland.

[2] https://eba.europa.eu/documents/10180/2522896/EBA+BS+2018+431+%28Draft+CP+on+Guidelines+on+ICT+and+security+risk+management%29.pdf

Comments of the European Financial Congress on proposals put forward in the consultation paper

The purpose of the Guidelines is to ensure a consistent approach in the EU single market, establishing requirements for mitigating and managing risks related to information and communication technologies (ICT), addressed to a broad and diverse group of financial market players. The implementation of the PSD2 Directive extends the use of information and communication technologies from well-regulated areas in the banking sector to new areas, the domain of non-banking institutions, many of which may not have as much experience in mitigating and managing ICT-related risks.

Considering the above, the draft Guidelines may be an important and significant document from the point of view of the financial sector, but, considering the customer's point of view, consumers may be its greatest beneficiary, due to the potential improvements in the security of financial services in the future.

1. **Do the Guidelines require clarification (for example, by indicating security standards relevant to a given area, etc.)?**

   Guidelines are usually a document of a general character, often containing specific recommendations. Since the draft Guidelines discussed here cover all EU member states and are addressed to organisations differing in the scale of their operations, it is not possible to create a detailed document, taking into account the specific nature of the operations of each of them.

   Nevertheless, one may consider supplementing the Guidelines, for example, by specifying Minimum Safety Standards (MSS) for individual categories of organisations or by making it clear to which organisations the Guidelines are addressed. In view of the wide variety of institutions and organisations covered by the Guidelines (from fintech startups to global banks), it seems important to clarify the principle of proportionality mentioned in item 4.1 of the draft Guidelines.

   In the opinion of some experts in the financial sector, it would be advisable to make the security standards more detailed by including direct references to examples of recognized standards in the field of ICT security. Because the Guidelines apply to the entire Community market, the "appropriate" level of detail can be achieved once the financial supervision authorities in each country have implemented them; the recommendations issued by the Polish Financial Supervision Authority are an example of this. Overly general Guidelines are open to interpretation both by organisations and by supervisors in each Member State.

2. **Do the Guidelines duplicate existing requirements contained in other regulations/recommendations addressed to payment service providers?**

   In terms of operations, the Guidelines aim to integrate all regulations concerning ICT and security management into a single legal text, addressed to all financial institutions and covering a wide spectrum of measures; however, it seems that the draft Guidelines do not meet this requirement. The draft selectively duplicates some regulations while ignoring others. Lack of consistency is evident, particularly in the context of the Guidelines on outsourcing, adopted after consultations on 25 February 2019.

   It would seem advisable to standardize all ICT Guidelines that are already in force and those currently being implemented, taking into account also guidelines issued by national regulators. This is important insofar as the national supervisory authorities will implement the final version of the Guidelines in their markets; therefore, it would be useful to take advantage of what has already been done. The Polish Financial Supervision Authority developed two detailed recommendations in areas addressed by the Guidelines. These are:

   - Recommendation D regarding the management of information technology and the security of the ICT environment in banks; and

   - Recommendation M concerning operational risk management in banks.

3. **Will compliance with the Guidelines be a heavy burden for the sector, and which organisations could be affected the most?**

   Meeting the requirements described in the Guidelines should not be a major problem for large banks. A significant proportion of the proposed Guidelines has already been implemented or is currently being implemented. Adapting to the requirements set forth in the Guidelines could be a significant problem for organisations operating on a small scale, such as cooperative banks and institutions offering payment services, and especially fintech startups. It is certainly not enough merely to invoke the principle of proportionality – as in the current draft of the Guidelines – without clarifying how this principle is to be applied, which aspects are important for these organisations and which are not. This applies in the first place to countries where "gold-plating" occurs. This can lead to other negative outcomes, such as migration of payment institutions to more "liberal" countries.

4. **Is there a risk that financial supervisors in different countries may adopt divergent interpretations of the Guidelines, which could lead to over-representation of applications filed with payment institutions in some countries (e.g. "mass registration" of fintechs in a country of choice, in order to come under supervision there, while operating in all other EU countries on the principle a single license)? What could be the consequences of such a trend?**

   The guidelines are merely recommendations, not a source of universally binding law, and compliance with these recommendations will depend on the interpretation and practice of local supervisors. The Guidelines could be a significant step towards

building a common level of requirements relevant to ICT security (the so-called common minimum level of playing field), but their general character and the principle of adequacy and proportionality leave plenty of room for interpretation. It seems certain that supervision authorities in various countries will differ as regards the scope of compliance enforcement, with some taking a more liberal approach to licensing and compliance of the organisations with the cybersecurity Guidelines, and others being more conservative. This, in turn, will encourage fintechs to register their business in countries where the supervisory authorities adopt a liberal approach. What is worse, the conservative approach is mainly adopted by the more developed supervisory authorities. As a consequence, clients in all member states may be exposed to a greater risk resulting from the single license principle. Payment institutions that potentially pose a threat to customers by registering in a country where the supervisory authorities adopt a liberal approach can operate within the EU across state borders on the basis of a single license. In contrast, "gold plating", which is practised by local regulators in some countries, will deter fintechs from applying for a payment institution license in member countries with conservative supervisors.

5. Do the Guidelines level off the playing field in the sector by establishing the same rules for all market participants?

The principle of proportionality included in the draft Guidelines severely limits the equalisation of opportunities for all market participants. On the other hand, it seems that it does equalise the opportunities on local markets, within specific categories of players (e.g. for banks or for TPPs in a given Member State). However, in the cross-border dimension, it is not possible for the rules to be identical even within one category of financial market participants, due to the risk of different interpretations of the Guidelines by national financial supervisors. Moreover, in the case of global institutions, it may not be possible for local, national branches to apply more restrictive rules than those used by the head office, subject to more liberal supervision.

6. Will the Guidelines affect the number of TPPs and the development of open banking?

It seems that in some Member State markets, compliance with the requirements of the Guidelines may become a barrier to entry and may have an impact on the number of TPPs and the growth of open banking. This may be especially true of those national markets where "gold plating" can be observed. Since the draft Guidelines contain arbitrary rules of adequacy and proportionality, a great deal depends on national supervisors. The requirements are quite general and can be interpreted either liberally or restrictively. In the latter case, a TPP may look for a more friendly Member State in which to apply for a license and then, under the terms of the single license, operate in all EU countries. In view of the above, it seems that the impact of the Guidelines on the number of TPPs and the growth of open banking will be rather insignificant.

7. **Is there a risk that some institutions may try to circumvent the requirements imposed by the Guidelines (e.g. by using low-quality collateral, etc.)? What could be the consequences of this?**

   While the implementation of the Guidelines may in general contribute to an improvement in ICT security of payment services, especially if industry MSS (Minimum Safety Standards) are adopted, there will always be the risk of deceptive compliance by some institutions. This could lead to fraud resulting from the implementation of PSD2. Should this trend escalate, it could trigger negative PR and slow down the growth of open banking.

   There is one rather important aspect of deceptive implementation of the Guidelines by institutions such as TPPs. In the case of fraud caused by TPP, consumers will blame the banks. Therefore, the banking sector may suffer the negative consequences of the operation of third parties, and may be exposed to loss of reputation and credibility, because the bank is responsible to the client. Mitigation of this risk may lead to increased costs and complexity of financial services security, to the detriment of convenience and user comfort.

   Systemic mitigation of risk could be accomplished by national regulatory policies and a system for auditing the supervised organisations, taking into account the principle of proportionality, including the level of risk of the impact of a given institution's non-compliance on the entire market. Tools in the form of sanctions (penalties) would enable regulators to counteract the operations of risk-generating organisations and to protect customers more effectively against the risk of fraud, and the banking sector against loss of credibility. Another way of mitigating the aforementioned risks is to apply industry standards, such as Open API (e.g. Polish API) and to use industry solutions, such as PSD2 hub, which bring in technology and ensure adequate security, while maintaining minimum security standards acceptable to the entire industry.

8. **Will users of payment services be significantly more secure after the implementation of the Guidelines or will there be no change? How will this affect the consumer?**

   Given the current regulations and the rather general nature of the Guidelines, it seems that they will not significantly improve security for users of payment services. Undoubtedly, the implementation of the Guidelines may make financial institutions more mature in the area of information technology management and ICT security, and this may translate into improved ICT security in the future. Nevertheless, one should not expect any significant improvement in this respect.

9. **Would supervisory sanctions for non-compliance with the Guidelines improve ICT security in the industry?**

   Regulation without sanctions plays only advisory role and can be treated as a set of good practices. Companies lack strong motivation to implement such regulations. Only the prospect of sanctions motivates the market to act. GDPR is a good example:

sanctions for failure to comply with personal data protection regulations mobilised all organisations that collect and process personal data.

The application of uniform sanctions will probably be hindered by the unequal treatment of payment institutions by the supervisory authorities of various countries. The uniform license allows service providers to operate in all EU countries, while the principle of home country supervision means that the operation of the payment institution in another EU Member State is subject to the banking supervision authority of the country which licensed the payment institution to operate. The home country is also responsible for supervising the operations of the payment institutions it has licensed. This means that the same institutions may be subject to different sanctions, depending on the payment institution's home country.

10. Will the Guidelines make it more difficult to use financial services?

Because the Guidelines are very general, their implementation should not make it more difficult for consumers to use financial services. The burden of implementing the Guidelines lies with the financial institution, but the obligation to comply with the Guidelines should not cause any serious difficulties for users of financial services.

11. Do the draft Guidelines cover all issues related to ICT and the management of security risk?

The authors of the Guidelines assume that the purpose of the document is to integrate all regulations pertaining to ICT and security management in one legal text, applicable to all financial institutions and a wide spectrum of measures; however, as already pointed out, the draft Guidelines do not meet this requirement. By analogy, this also means that all issues concerning ICT and security risk management should be treated exhaustively. It seems that the proposed regulation is based on the classic separation of the “business” and “IT” functions within the organisation, and fails to take into account new configurations, represented in particular by fintech startups. The proposed draft Guidelines may be criticised for ignoring new developments in IT, such as cloud computing and DLT. In the area of management, it seems that the proposed regulation does not take into account rather common methodologies of software development, based on iterative-incremental software development (the agile methodology). The proposed approach to acquiring and developing systems is closer to the traditional “waterfall” model. In conclusion, the Guidelines do not address all important issues relevant to the specific nature of TPP organizations operating in the open banking segment.

Experts believe that the criteria for inclusion in the Guidelines are unclear and there is no top-down approach – which makes it difficult to verify the extent to which the proposed regulations exhaust issues relevant to risk management related to ICT security. According to some experts, the Guidelines also ignore the important issues of end-to-end data encryption in the course of data processing; access to data, which conflicts with banking confidentiality (GDPR); management of ICT security in the form of internal outsourcing, etc.

12. **Are all definitions and concepts clear and comprehensible?**

    The definitions used in the draft Guidelines are fairly clear and comprehensible, but the draft itself does not cover all issues of systemic and operational risk management related to ICT.

13. **Are the security requirements proposed in section 4.4 clear? Have any been omitted?**

    The security requirements proposed in section 4.4 are comprehensive and constitute a base, which can be further elaborated by financial institutions, taking into account the ICT risks they have identified. Overly detailed Guidelines could become obsolete within a short space of time.

14. **Are the requirements concerning change management clear? Which seem to be the most important?**

    In general, the requirements for change management as defined in section 4.6. are clear. They take into account the most important control mechanisms in the process of change management, software development and project implementation. It seems that in section 4.6. ICT Project and Change management, it would be advisable to add a provision on the use of control mechanisms regardless of the methodology employed. According to experts, the provision in section 4.6.2 ICT systems acquisition and development, item 74, also requires modification. Its literal meaning may suggest that the use of agile methodologies in software development is not compliant with the Guidelines.

15. **Should the principle of proportionality be applied to the business continuity management specification proposed in Section 4.7?**

    The principle of proportionality applies to all requirements included in the draft Guidelines. A system for business continuity management is built on Business Impact Analysis (BIA), which enables the identification of critical processes, for which appropriate mechanisms should be in place to ensure business continuity. Depending on the scale of operations and the size of the enterprise, in accordance with the principle of proportionality, the analysis should provide information on the requirements for business continuity management.

16. **Should Subsection 4.3.2 of the draft Guidelines link the review of processes, functions and resources to the review of the framework for risk management (define the minimum frequency of the review of processes, functions and resources)?**

    It seems that in Section 4.3.2 of the draft Guidelines, which deals with the review of processes, functions and resources, the provision on the minimum and maximum frequency of the review of processes, functions and resources should be elaborated, or a new provision should be added, to the effect that such a review is necessary in case of significant changes in resources, infrastructure, systems or processes.

17. **Should a minimum audit frequency be specified in subsection 4.3.6 of the draft Guidelines?**

    It seems that quantitative requirements concerning the minimum and maximum audit frequency should be imposed, provided the bracket is sufficiently wide (for example, from once a year to once every 3 years), in order to accommodate the specific nature of the operations of any given organisation.

18. **Is it realistic to require – as in Subsection 4.4.7 – that all types of POS devices be tested (for example, how can a PSP test mobile devices, that is, all models of smartphones on which a mobile terminal can be installed, e.g. mPOS, softPOS, Fastpass, etc.)?**

    It seems that the draft recommendation in its present form does not take into account the current trends in payment services technology. Item 50 of Section 4.4.7. Information security reviews, assessment and testing, requires all payment service providers to test security measures implemented in payment terminals and devices used to provide payment services, payment terminals and devices used to authenticate the user of payment services, and devices and software supplied by the payment service provider to the user of the payment service to enable the user to generate/receive an authentication code. In the case of mobile devices, such as smartphones, tablets, etc., the requirement to test each device model is not unrealistic, but it may be considered excessively burdensome. Therefore, testing could be restricted to a limited range of models, reducing the potential choice of compliant mobile devices. It is suggested that the requirement to test mobile devices (smartphones, tablets, etc.) be limited to the testing of the operating system only (e.g. Android, iOS, Windows Mobile, etc.).