Contribution of BaFin to the European Commission's consultation document „FinTech: A more Competitive and Innovative European Financial Sector"

1. Fostering access to financial services for consumers and businesses

1.2. Is there evidence that automated financial advice reaches more consumers, firms, investors in the different areas of financial services (investment services, insurance, etc.) and at what pace? Are these services better adapted to user needs? Please explain.

We observe that many providers of automated financial advice only grow slowly in terms of customers and AuM.
With regard to cooperation between the providers of automated financial advice (tools) and other firms, we observe increasing cooperation. Some providers offer their tools to other investment firms who themselves provide some kind of automated advice.
Most providers aim to better adapt their services to user needs such as customer-friendly communication, comprehensiveness etc. through simpler and informal language and customer-friendly surfaces, etc. To BaFin's knowledge, this is appreciated by most customers.
With regard to user needs such as customer protection, suitable investment products etc., some providers have difficulties to adjust their platforms and services to a MifID-compliant format. This is in particular relevant if the service provided qualifies as investment advice or portfolio management under MiFID. The assessment of the clients' knowledge and experience, their risk-notion and their financial situation has to cover all relevant aspects and firms have to ensure that the information provided by clients is consistent. Finally, the underlying algorithms have to be designed to provide suitable investment recommendations/investment strategies.
Further, providers of automated financial advice have to take into account several other aspects with regard to client needs: Investors tend to overestimate their theoretical knowledge about financial instruments and also tend to overestimate their risk-notion.
On the other hand, automated financial advice platforms often are less costly than traditional investment services and offer consumers access to a wide range of products.

1.4. What minimum characteristics and amount of information about the service user and the product portfolio (if any) should be included in algorithms used by the service providers (e.g. as regards risk profile)?

The minimum characteristics and the amount of information which should be included in the algorithm depends on the different business models. For investment advice services a suitability test, and for non-advisory investment services an appropriateness test need to be implemented into the algorithm.
For the appropriateness test the algorithms needs to collect certain information such as knowledge and experience with regard to doing business with certain types of financial instruments or investment services and evaluate this information.

Additionally, for the suitability test the algorithm needs to query and assess the investment objective, the risk appetite and the risk-bearing capacity (financial conditions) of each individual service user.
The algorithms' underlying scoring system for the suitability and appropriateness test is vital and needs to be robust and less prone to errors. Legal requirements such as providing a consultancy record (§34 Abs. 2a WpHG) must be met.
Further, the algorithm must be designed in such a way that flaws in the functioning of the tool due to errors, hacking or manipulation of the algorithm are mitigated. Risks to consumers related to flaws in the functioning of the tool, such as consumers making unsuitable decisions because of limitations or assumptions within the tool must be mitigated, too. The algorithm must be reviewed and updated in this respect on an ongoing basis.

1.5. What consumer protection challenges/risks have you identified with regard to artificial intelligence and big data analytics (e.g. robo-advice)? What measures, do you think, should be taken to address these risks/challenges?

As an integrated supervisory authority our focus lies on the financial stability of financial institutions as well as on consumer protection issues.
We have recognized several risks for consumers stemming from new data analytic technologies. We have identified such risks as price discrimination, access to and/or exclusion from services, quality of products and services and cyber risks. Overall, we support the risks identified in the JC discussion paper on the use of Big Data by financial institutions because our authority also made its contributions to this paper. Additionally, we have identified the following risks:

- Infringement of right of informational self-determination: Some types of attractive insurance products might only be available for policyholders, who agree to be monitored to a certain extent.
- Additionally, consumers might not fully understand the consequences of opting-in to use of their personal data.
- More generally spoken we also see a risk that trust in the financial system is undermined if data is misused on a large scale.

1.10. Are there already examples of price discrimination of users through the use of big data? Can you please provide examples of what are the criteria used to discriminate on price (e.g. sensor analytics, requests for information, etc.)?

We have yet not come across any direct cases of price discrimination.

2. Bringing down operational costs and increasing efficiency for the industry

2.5. What are the regulatory or supervisory obstacles preventing financial services firms from using cloud computing services? Does this warrant measures at EU level?

According to German legislation for the use of cloud computing services the same legal requirements apply as to any other services that financial services firms obtain from third parties.

2.6. Do commercially available cloud solutions meet the minimum requirements that financial service providers need to comply with? Should commercially available cloud solutions include any specific contractual obligations to this end?

We refer to the ongoing consultation on recommendations on outsourcing to cloud service providers on EBA-level (https://www.eba.europa.eu/regulation-and-policy/internal-governance/recommendations-on-outsourcing-to-cloud-service-providers).

2.7. Which DLT applications are likely to offer practical and readily applicable opportunities to enhance access to finance for enterprises, notably SMEs?

In the finance sector, our impression is that the first DLT applications which offer opportunities for enterprises will be in niches, especially back office applications. DLT may also have the potential to achieve superior propositions for cross-border payments and trade finance.
In addition micro-payments might be considered an opportunity for DLT, in connection with relevant developments in the industry (eg Internet-Of-Things, energy sector).
Another future opportunity for SMEs might be to track, trade and issue stocks, bonds and other assets.

2.8. What are the main challenges for the implementation of DLT solutions (e.g. technological challenges, data standardisation and interoperability of DLT systems)?

In terms of technological challenges with regard to financial services, it cannot be taken for granted that DLT solutions will have the capability to replace market infrastructures which are processing very high volumes (Bitcoin 7 trx per sec / Visa 50k+ trx per sec). Not only in public applications like Bitcoin, but also in private blockchains it might prove difficult to use DLT in cases where high transaction volumes have to be processed. The proof of sufficient scalability would seem to be one of the main challenges when it comes to surmounting this shortcoming.

An additional challenge is the security of DLT solutions. While many observers praise DLT technology for its avoidance of a single point of failure, it could also bring about heightened risk due to multiple point attacks. In addition, forward security describes what is needed, and this is currently not given. Most DLT solutions are using complex hash algorithms, but there is no guarantee that the hash functions cannot be reversed in the future.

Currently, it seems that several banks and institutions are developing their own DLT solutions. However, this creates segregation and various interfaces and might restrict DLT's potential.

One challenge that has been observed on several occasions is that governance is lacking in some decentralised systems and that this missing governance is raising several issues. For example, a comprehensive and efficient risk management requires a strong governance and

appropriate decision-making processes must be available to make decisions in time for future developments.

What can be considered as a medium-term challenge is the need to define standards for DLT applications. Standardisation has already started in the industry under the aegis of ISO on a worldwide basis. For this reason, no regulatory activity is necessary in Europe at the moment.

Furthermore the main challenges include but are not limited to technology risk, cryptological risk, risk of economic efficiency of the technology and operational embedding into current business processes and practices.

2.9. What are the main regulatory or supervisory obstacles (stemming from EU regulation or national laws) to the deployment of DLT solutions (and the use of smart contracts) in the financial sector?

DLT solutions serve as the technological basis for business cases, so they do not need different regulatory approaches per se. From our perspective, the regulatory approach should be neutral with regard to technology. Regulators should focus their attention on the potential risk of the business model. This needs to fit into the legal frameworks and comply with existing EU regulatory requirements. Only if the application of DLT alters the risk(s) of the business model the regulatory approach might need to be adopted.
Regarding the treatment of smart contracts within the respective legal frameworks, there still seems to be some uncertainty. In general, smart contracts are part of a DLT solution (decentralized public ledgers) as these set up the rules and rights within the DLT system and the participating members. From a legal perspective a smart contract can effectively be nothing more than a piece of software code, it therefore has to be considered differently than a paper-based contract with regard to its legally binding character. Clarifying the legal status of smart contracts as well as of assets transferred and/or stored via DLT technology is a challenge to be tackled by the legislator in the near future.

Another open question is the responsibility for data security / data privacy with regard to the information potentially shared in the ledger.

2.10. Is the current regulatory and supervisory framework governing outsourcing an obstacle to taking full advantage of any such opportunities?

We do not regard the current regulatory and supervisory framework governing outsourcing as an obstacle to take advantage of efficiency opportunities but rather as a necessary and reasonable framework to ensure the sound management of any outsourcing activities by financial services firms.

2.11. Are the existing outsourcing requirements in financial services legislation sufficient? Who is responsible for the activity of external providers and how are they supervised? Please specify, in which areas further action is needed and what such action should be.

Responsibility for the activity of external providers remains with the financial services firm with respect to the outsourced activities. Supervision of external providers is primarily indirect being part of the supervision of the financial services firm. Additionally German legislation empowers BaFin to conduct on-site inspections on the premises of the external provider with respect to those activities that a financial services firm has outsourced.

3. Making the single market more competitive by lowering barriers to entry

3.1. Which specific pieces of existing EU and/or Member State financial services legislation or supervisory practices (if any), and how (if at all), need to be adapted to facilitate implementation of FinTech solutions?

Notwithstanding implementation of current European initiatives, at the moment BaFin does not see a need for an adaption of European or national legislation or supervisory practice to facilitate the implementation of FinTech solutions. From our point of view various national and European laws and regulations ensure robust supervision of the financial sector while not stifling innovation as they are worded in a technology neutral way. Moreover, up to now we have not seen any business models which could not be subsumed under the existing laws and regulation. When assessing whether a FinTech business model is subject to the licensing procedure and the respective ongoing supervision, we are looking at the specific business activity of a FinTech company regardless of the underlying technology or how the business is conducted (digital or analogue). Equal treatment and clear rules create trust for consumers as well as for other market players. However, there are FinTech activities which do not fall within the scope of the current European or national regulatory framework and subsequently are not subject to supervision. For the time being we regard this as appropriate because we have not identified any new risks caused by those unregulated FinTech activities that would require regulation.
Where it was deemed necessary, well-chosen and specific regulatory adaptions have been and should be implemented to foster digitalisation (e.g. video identification). But, since digital innovation has to be sustainable, proven standards like data protection regulations (in the context of financial services) should not be lowered in favour of easier market access for FinTech-companies.

3.2. What is the most efficient path for FinTech innovation and uptake in the EU? Is active involvement of regulators and/or supervisors desirable to foster competition or collaboration, as appropriate, between different market actors and new entrants. If so, at what level?

As there might be a potential conflict of interests between fostering competition and the mandate to ensure integrity of financial markets and protect consumers, from our point of view an active involvement of regulators and/or supervisor to foster competition might not necessarily be appropriate. For the reason of avoiding potential conflicts of interest, most competent authorities do not have the mandate to promote or to foster competition. To our knowledge only the UK conduct authority – FCA – has such a mandate. Most competent authorities have the

mandate to protect financial stability as well as to protect consumers. In any case promoting FinTech solutions must not lead to a race-to-the-bottom in regulatory standards.

3.3. What are the existing regulatory barriers that prevent FinTech firms from scaling up and providing services across Europe? What licensing requirements, if any, are subject to divergence across Member States and what are the consequences? Please provide details.

From our point of view no barriers are created by the existing regulatory framework, which would prevent FinTech firms from scaling up and providing services across Europe.

3.4. Should the EU introduce new licensing categories for FinTech activities with harmonised and proportionate regulatory and supervisory requirements, including passporting of such activities across the EU Single Market? If yes, please specify in which specific areas you think this should happen and what role the ESAs should play in this. For instance, should the ESAs play a role in pan-EU registration and supervision of FinTech firms?

At the moment we do not see the necessity for the introduction of new licensing categories for FinTech activities, including passporting of such activities across the EU Single Market. First of all there is no concrete definition as to what constitutes a FinTech. The existing FinTech definitions such as the ones from the FSB or ECB are rather broad and therefore prone to cause uncertainties as to what is considered to be a FinTech. Second, there are good reasons, why current regulatory and supervisory frameworks are worded in a technology neutral way and provide a catalogue of regulated activities (regardless how they are conducted – analogue or digital) and not technologies. Due to the rapid development of digital technology a regulatory framework which would regulate only the technology itself might be outdated by the time it would come into force or would be implemented. Third, as described in the answer to 3.1 we have not seen a FinTech business model yet which could not be subsumed under the existing laws and regulation. Therefore a separate licensing category should only be established if there are new and unregulated risks exclusively caused by the FinTech business models and if this cannot be solved by an amendment of the current technology neutral regulation. In that case, any possible registration and supervision should take place by the supervisory authorities that would be responsible for the registration and supervision of non-FinTech regulated activities.

3.5. Do you consider that further action is required from the Commission to make the regulatory framework more proportionate so that it can support innovation in financial services within the Single Market? If so, please explain in which areas and how should the Commission intervene.

At the moment we do not see the need for an intervention by the Commission to make the European regulatory framework more proportionate with regard to supporting innovation in financial services. In general the principle of proportionality should be applicable to all regulated entities (not only FinTechs) and reflect the risk profile of the respective entity (risk based approach).

3.7. Are the three principles of technological neutrality, proportionality and integrity appropriate to guide the regulatory approach to the FinTech activities?

Yes.

3.8. How can the Commission or the European Supervisory Authorities best coordinate, complement or combine the various practices and initiatives taken by national authorities in support of FinTech (e.g. innovation hubs, accelerators or sandboxes) and make the EU as a whole a hub for FinTech innovation? Would there be merits in pooling expertise in the ESAs?

Achieving a coordinated approach to regulatory and supervisory treatment of innovative financial activities should be a primary goal of the ESAs in accordance with Article 9(4) of the ESA-Regulations. At the same time arrangements at the lowest level, i.e. a “race to the bottom”, should be avoided.

3.10. Are guidelines or regulation needed at the European level to harmonise regulatory sandbox approaches in the MS? Would you see merits in developing a European regulatory sandbox targeted specifically at FinTechs wanting to operate cross-border? If so, who should run the sandbox and what should be its main objective?

There is certainly a trade-off between the desire to foster the development of FinTechs on the one hand and consumer protection and financial stability on the other hand. Therefore, it is still unclear whether sandboxes are desirable at all. The proportionality principle applies to all regulated entities. The risk profile of an entity needs to be reflected both by its risk management and by the supervisor (dual proportionality). The concept of “same business – same risk – same rules”, also known as a “level playing field”, has proved successful and is being applied to licensed FinTech entities in the same way as to “traditional” entities. The dual proportionality principle therefore allows us to ensure a level-playing field without stifling innovation. Nonetheless, if the technical innovations applied by the FinTech entity alter its risk profile, the supervisory intensity will be adjusted to match. Since start-ups are often small in size and interconnectedness, they will usually have a relatively low risk profile and therefore are usually supervised less intensively than major institutions. It can be noted that there should be a common understanding to what extent sandboxes are permitted by European laws and regulations.

3.12. Is the development of technical standards and interoperability for FinTech in the EU sufficiently addressed as part of the European System of Financial Supervision? Is the current level of data standardisation and interoperability an obstacle to taking full advantage of outsourcing opportunities?

Regarding the first part of the question, BaFin acknowledges the European Commission's recent initiatives to increase harmonisation in the context of legal reporting requirements. Notwithstanding that, BaFin would like to clarify that in its view, the European System of Financial Supervision should try to avoid developing low-level technical specifications for industry standards. Rather, BaFin believes that, except where it is essentially necessary for exercising their mandate, these bodies should seek to confine themselves to publishing only rather general recommendations and/or legal requirements for technical industry standards. Since the increasingly technical set-up of financial services seems to make the timely agreement of technical specifications necessary in more and more cases, a way has to be found to foster these procedures. In this respect it has to be considered whether some lessons learned can be adopted from other industries, including telecommunications.

3.15. How big is the impact of FinTech on the safety and soundness of incumbent firms? What are the efficiencies that FinTech solutions could bring to incumbents? Please explain.

The impact of Fintechs on safety and soundness of incumbents very much depends on how far they are complements or competitors. Fintechs enable banks to introduce new technology faster and experiment with new kinds of service provision. This may allow them to rationalize their back office in a more efficient way. Revenues may increase if Fintechs enable banks to better cater for the specific needs of their customers. However, the integration of external providers or the outsourcing of IT-System to Fintechs may also increase banks' vulnerabilities and exposure to operational risk.
Moreover, Fintechs generally operate in core segments of banks' businesses (e.g. payments, investments etc.) by either being a cooperation partner of incumbent institutions or their direct competitor. This may put pressure on bank revenues.
FinTech also introduces new players and solutions into the asset management sector and hence, could increase diversification, contingent upon the diversity of business models offered. The fact that FinTech investment advice and management, e.g. in the form of robo advice, is largely automated with limited personal interaction, means that FinTech can have a potential cost advantage over traditional portfolio advisors. This, in turn could put pressure on incumbents to reduce costs and lower pricing, which might be efficiency enhancing with regard to the financial system as a whole.
In addition, platform-based advice could enhance transparency and reduce information asymmetries as well as principal agent problems depending on how the process of translating the customer information given into a portfolio proposal and the final investment decision is set up. FinTech could also facilitate access to investment advice and portfolio management services for consumers as platform-based models tend to operate with low minimum investment amounts and offer convenient access via mobile and internet platforms.
On the other hand, rising levels of automation in the asset management sector might imply financial stability risks associated with unidirectional portfolio shifts or herding behavior. In terms of operational risks, interdependencies among different institutions and cyber risks could become more prominent.

4. Balancing greater data sharing and transparency with data security and protection needs

4.2. To what extent could DLT solutions provide a reliable tool for financial information storing and sharing? Are there alternative technological solutions?

There is no doubt that any kind of storing or sharing of financial information presents very high requirements in terms of security aspects such as confidentiality, availability and integrity. In public DLT systems, conclusive analysis will be needed to ascertain whether strong confidentiality is guaranteed or not. DLT solutions spread data over several nodes, which makes the system invulnerable against data loss. Furthermore, due to the consensus algorithms, data integrity is ensured, at least if not the relevant (authorised) nodes or a specific majority (e.g. more than half of the nodes) are compromised. Leaving aside the fact that the cryptography might not be strong enough, DLT solutions can be a reliable tool for storing and sharing financial information, especially in the case of private DLT solutions with strict access control. However, storing data on a DLT comes at a specific risk. As indicated above, (cf. response to question 2.8.), some scientists are predicting that in the future it might be possible to decrypt the cryptography which is currently used. Data might be encrypted today, but all this encrypted data of today will be accessible to every node in the network. Therefore, every connected node can make copies of today's encrypted data and can potentially decrypt it with tomorrow's technology. This effect alone carries a high risk, depending on the risk appetite of the organization using the DLT technology. If the specific business of a bank requires for instance a perimeter protection a DLT solution may not be possible. One possible scenario could be to use DLT solutions to only store corresponding hash values of data inside the DLT and not the data itself. As alternatives for DLT solutions, depending on the use case, many centralised applications are still state-of-the-art in BaFin's view. Nevertheless information sharing between all parties of a DLT solution might offer almost real-time availability of the information and access to reliable data/ information through storing and sharing data in a single reliable distributed ledger. As a result legacy solutions /systems which currently require ongoing reconciliation between the systems of the interacting market participants as well as backup capacities for the stored data could become redundant.

4.3. Are digital identity frameworks sufficiently developed to be used with DLT or other technological solutions in financial services?

From our perspective, there are no digital identity frameworks that are mature enough to be used in DLT solutions. However, EU regulations like eIDAS seem to be a good approach, but their productive usage is still not widespread. Creating a common framework under eIDAS at an EU level is only partially helpful since DLT solutions will not be confined to an EU-wide range. There is a backlog of digital identity frameworks with international interoperability.

4.4. What are the challenges for using DLT with regard to personal data protection and how could they be overcome?

With regard to legal requirements for IT-security authorised companies have to comply with the provisions to data security and data integrity. As part of this framework personal data has to have a high level of protection regardless of the technology used..

The purpose of data protection is to protect the individual's right to privacy being impaired through the handling of his/her personal data which means any information concerning the personal or material circumstances of an identified or identifiable individual. One way to achieve this could be to render any type of personal data anonymously. Another way could be to use a DLT/Blockchain solution that offers privacy and selective transparency of transactions.

4.7. What additional (minimum) cybersecurity requirements for financial service providers and market infrastructures should be included as a complement to the existing requirements (if any)? What kind of proportionality should apply to this regime?

We regard cybersecurity of individual market actors and financial market infrastructures as an absolute necessity in order to ensure safety and soundness of the overall financial industry.

In general, principles are risk based.
Regarding financial market infrastructures we have a specific view: The business models and the business continuity needs of financial market infrastructures (FMIs) are significantly distinct from those of financial service providers. Specific cyber attack patterns tailor-made for targeting FMIs may thus differ from the ones which are targeting other financial market entities. It should be up to supervisors and overseers of FMIs to lay down the requirements for different types of FMIs specifically while considering proportionality and recommendations agreed at international level (e.g. Cyber guidance of CPMI/IOSCO).
Regarding banking supervision, the CRD IV is implemented by the German banking law (Kreditwesengesetz, KWG) and the Minimum Requirements for Risk Management (Mindestanforderungen an das Risikomanagement, MaRisk). Accordingly, financial institutions shall have inter alia a sound and effective risk management.
MaRisk stresses that a sound and effective risk management must include also the technical and organisational resources. These resources shall be based on the internal operating needs, business activities and risk situation.
Furthermore, MaRisk requires that IT systems (hardware and software components) and the related IT processes shall ensure the integrity, availability, authenticity and confidentiality of the data. To this end, generally established standards shall apply to the arrangement of the IT systems and related IT processes […]. Examples of such generally established standards are the ISO 2700x series or the "IT-Grundschutz" that is issued by the Federal Office for Information Security (Bundesamt für Sicherheit in der Informationstechnik, BSI).
Furthermore, the BaFin circular "Banking Supervision Requirements for IT"(Bankaufsichtliche Anforderungen an die IT, BAIT), which is currently under public consultation, further refines the supervisory expectations as laid down in the KWG and the MaRisk regarding information and communication security.

Moreover, the national implementation of the PSD II via the Payment Services Supervision Act (Zahlungsdiensteaufsichtsgesetz, ZAG) replaces the existing requirements for payment service providers. The already existing incident reporting framework towards the national competent authority will be adjusted and maintained.
Furthermore, with the national legislation that implements the Directive on security of network and information systems (NIS directive) via the IT security law (Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme , IT-SIG), critical infrastructures must have appropriate organizational and technical measures in place to avoid breaches of availability, integrity, authenticity and confidentiality of all IT systems, components or processes, which are essential for the functioning of their operated critical infrastructures.
Given this triad we regard the requirements for cybersecurity for financial service providers currently as sufficient and see no immediate need for additional cybersecurity requirements.
Financial institutions that have to comply with KWG and MaRisk are subject to a risk-based approach, taking into account the proportionality of legislative and supervisory actions to risks and materiality of risks.
However, as cyber risks are rapidly developing in complexity, including where FinTech might facilitate interconnectedness of systems and an increase in the number of points of access to core parts of the financial system, and as are using increasingly innovative methods to compromise systems are used it must be ensured that the regulatory framework is keeping pace with the ongoing evolution of cyber risks. If changes to the regulatory framework occur, it needs to be adjusted in a timely manner.
Regarding insurance supervision, the Solvency II framework is implemented by the German Act on the Supervision of Insurance Undertakings (Versicherungsaufsichtsgesetz, VAG) and the Delegated Regulation (EU) 2015/35. According to this, insurance undertakings also have to install a sound and effective risk management. They have also to maintain security, integrity and confidentiality of information. But in comparison to the banking sector, there is no additional circular like the MaRisk which contains more detailed supervisory requirements.

4.8. What regulatory barriers or other possible hurdles of different nature impede or prevent cyber threat information sharing among financial services providers and with public authorities? How can they be addressed?

BSI, BaFin and Deutsche Bundesbank are in close contact with each other and share information with respect to cyber related incidents. Moreover, there are areas in which the three agencies work together in the development of requirements for financial service providers.

In some countries, data protection issues might be a legal barrier to cyber threat information sharing. Financial services providers might also be afraid of sharing information amongst themselves or with regulators because they could fear this would lead to the disclosure of business secrets. Furthermore, being too transparent in disclosing successful attacks might induce reputational risks and inspire criminals to threaten other entities using the particular attack vector. Regulated entities could be inclined to withhold weaknesses to the competent authority as they could face sanctions.

Besides that, we see no obstacles that would impede or prevent cyber threat information sharing among public authorities. Certain limitations to the sharing of any information, however, may arise due to different responsibilities of the various authorities.

These concerns and potential hurdles could be addressed by establishing a strict confidentiality regime providing harsh sanctions for illegal breaches of confidentiality. Besides that, ISO 27032 is suitable to facilitate information sharing.

For the further background on the reporting frameworks we refer to question 4.7.

4.9. What cybersecurity penetration and resilience testing in financial services should be implemented? What is the case for coordination at EU level? What specific elements should be addressed (e.g. common minimum requirements, tests, testing scenarios, mutual recognition among regulators across jurisdictions of resilience testing)?

We regard penetration testing and resilience testing as two very important prerequisites for information and communication security and availability of financial services. European harmonization could help to create a minimum-level of cybersecurity in financial services across Europe. However, supervisory resources, skills and capabilities must be adequate to ensure the enforcement of such harmonized rules. As there is no such thing as a purely national cyber risk because of its genuine network dimension supervisory cooperation and communication is key, again.

MaRisk (refer to question 4.7) requires financial institutions to have plans for contingencies affecting time-critical activities and processes (contingency plans). The measures detailed in the contingency plan shall be aimed at reducing the extent of any potential damage and therefore incorporate cybersecurity aspects as well. In the insurance sector, there are similar requirements.

Regular contingency tests shall be carried out in order to verify the effectiveness and suitability of the contingency plans. The results of the contingency tests shall be communicated to the respective responsible staff.

In the case of outsourced time-critical activities and processes, the outsourcing institution and the service provider shall have mutually coordinated contingency plans.

Beyond that, financial institutions are expected to have protective measures against cyber-attacks in place such as,

- *Careful planning, safeguarding and monitoring of IT systems and networks*
- *Testing of IT systems and processes for security loopholes, for example by way of audits, vulnerability scans or penetration tests*
- *Effective patch management that ensures in particular that security-related software up-dates and any configuration changes that may be required are carried out in a timely and secure manner*
- *Security measures in software development*

- *Taking due account of IT security in the outsourcing of activities and the purchasing of IT systems*

Hence, institutions are expected to conduct penetration or resilience testing proportional to their exposure to information and communication risks arising from cyber threats.

While considering our answer to Q4.7 with regards to FMIs, a mutual recognition regime for the requirements of different national and European regulators might be essential and an important building block for a resilient financial market ensuring a minimum security level. Being too prescriptive with regards to minimum requirements, tests, and testing scenarios might reduce flexibility of competent regulators in reacting to a changed threat landscape and adapting to the specific needs of particular FMIs.