JC 2019 25

10 April 2019

Joint Advice of the European Supervisory Authorities

To the European Commission on the costs and benefits of developing a coherent cyber resilience testing framework for significant market participants and infrastructures within the whole EU financial sector

Introduction and legal basis

1. On 8 March 2018, the European Commission (Commission) published its *FinTech Action Plan*[1]. In the Action Plan, the Commission invited *'[…]the ESAs to evaluate, by Q4 2018, the costs and benefits of developing a coherent cyber resilience testing framework for significant market participants and infrastructures within the whole EU financial sector.'*

In this context, the Commission considered *'[…] the efforts that the ECB, the ESAs and national supervisors are making for example to develop an EU-wide Threat Intelligence Based Ethical Red Teaming (TIBER-EU) testing framework as promising.'*

2. The European Banking Authority (EBA) competence to deliver an opinion is based on Article 56 in the context of its tasks in Chapter II and more in particular of Article 34(1) of Regulation (EU) No 1093/2010[2] as cyber-resilience in the EU financial sector relates to the EBA's area of competence.

3. The European Insurance and Occupational Pensions Authority (EIOPA) competence to deliver an opinion is based on Article 56 in the context of its tasks in Chapter II and more in particular

[1] COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN CENTRAL BANK, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS FinTech Action plan: For a more competitive and innovative European financial sector. COM/2018/0109 final. Available at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52018DC0109

[2] Regulation (EU) No 1093/2010 of the European Parliament and of the Council of 24 November 2010 establishing a European Supervisory Authority (European Banking Authority) amending Decision No 716/2009/EC and repealing Commission Decision 2009/78/EC (OJ L 331, 15.12.2010, p. 12)

of Article 34(1) of Regulation (EU) No 1094/2010[3] as cyber-resilience in the EU financial sector relates to the EIOPA's area of competence.

4. The European Securities and Markets Authority (ESMA) competence to deliver an opinion is based on Article 56 in the context of its tasks in Chapter II and more in particular of Article 34(1) of Regulation (EU) No 1095/2010[4] as cyber-resilience in the EU financial sector relates to the ESMA's area of competence.

General comments and proposals

5. As noted in the *FinTech Action Plan*, the cross-border nature of cyber threats requires a high degree of alignment of national regulatory and supervisory requirements and expectations. As the financial sector becomes increasingly dependent on digital technologies, ensuring its resilience while tackling ever-growing cyber threats is becoming an important concern of the Commission. Cybersecurity risks undermine confidence and represent a threat to the stability of the EU financial system.

6. The Commission has also noted the emergence of different regulatory mandated or sponsored cyber resilience testing frameworks. These efforts require facilitation, synchronisation and cooperation, in order to avoid increased risks, costs, duplication of work and additional burden for financial market participants and infrastructures within the EU financial sector.

7. The three ESAs welcome the opportunity to provide the Commission with advice on the 'costs and benefits of developing a coherent cyber resilience-testing framework for significant market participants and infrastructures within the whole EU financial sector'.

8. The ESAs believe that cooperation between the relevant stakeholders based on a coherent cyber resilience-testing framework for significant market participants can support good and consistent risk management across the financial sector in relation to cyber security. This should in turn help ensure effective delivery of financial services across the EU while supporting consumer and market trust.

9. The ESAs are delivering the advice on a coherent cyber resilience framework through their Joint Committee, reflecting the fact that many aspects of cybersecurity are cross-sectoral.

10. The Boards of Supervisors of the three ESAs have adopted this Joint Advice on the basis of their respective rules of procedure. All three ESAs jointly conducted an analysis and agree on the main policy recommendations. However, the details of the application of a coherent

[3] Regulation (EU) No 1094/2010 of the European Parliament and of the Council of 24 November 2010 establishing a European Supervisory Authority (European Insurance and Occupational Pensions Authority) amending Decision No 716/2009/EC and repealing Commission Decision 2009/79/EC (OJ L 331, 15.12.2010, p. 48)

[4] Regulation (EU) No 1095/2010 of the European Parliament and of the Council of 24 November 2010 establishing a European Supervisory Authority (European Securities and Markets Authority) amending Decision No 716/2009/EC and repealing Commission Decision 2009/77/EC (OJ L 331, 15.12.2010, p. 84)

cyber resilience testing framework may vary both between and within sectors, depending on i) the cyber security maturity level of the market participants, ii) the systemic importance of the specific sectors, iii) the criticality of the service provided by the market participants and infrastructures, and/or iv) the national cybersecurity strategies for certain critical relevant entity[5] and infrastructures.

11. The ESAs understand that cyber resilience testing covers a wide variety of tools and actions, ranging from a basic level of security testing to threat intelligence led penetration testing (TLPT) where relevant entities are cyber mature enough to carry out such tests. This needs to be done by all relevant entities in such a way that is proportionate to and takes into account the relevant entities' size, their internal organisation, the nature, scope, complexity and riskiness of the services and products that the relevant entities provide or intend to provide.

12. For example, the draft EBA Guidelines on ICT and security risk management[6] specify that relevant entities should perform a variety of different information security reviews, assessments and testing, so as to ensure effective identification of vulnerabilities in its ICT systems and ICT services. Specifically, relevant entities may perform a gap analysis against information security standards, compliance reviews, internal and external audits of the information systems, or physical security reviews. Furthermore, the relevant entities should foster source code reviews, penetration tests, or red team exercises. Relevant entities should establish and implement an information security testing framework that validates the robustness and effectiveness of the information security measures and ensure that this framework considers new threats and vulnerabilities, identified through threat monitoring and the ICT risk assessment process.

13. The ESAs acknowledge that the fundamentals of cyber resilience testing needs to be done at relevant entity level. However, the most advanced type of testing – threat led penetration testing – could benefit from EU-wide coordination[7]. Coordination at relevant entity, group-level or country level could also be envisaged. The joint ESAs Advice, however, does not cover all types of security testing, but discusses only threat led penetration testing.

14. Furthermore, as a number of EU Member States have implemented or are currently implementing frameworks for cyber resilience testing[8], the establishment of a common set of guidance for such tests is necessary to ensure coherent application and the mutual acceptance of the results of these frameworks. This guidance would also create a level-playing field on cyber resilience for regulated entities and infrastructures within the EU.

[5] For the purposes of this Opinion, references to 'relevant entities' include 'financial institutions' within the meaning of Article 4(1) of the EBA Regulation and insurance and reinsurance undertakings addressed by the EIOPA Regulation as well as 'financial market participants' within the meaning of Article 4(1) of the ESMA Regulation.

[6] Guidelines on ICT and security risk management, https://eba.europa.eu/regulation-and-policy/internal-governance/guidelines-on-ict-and-security-risk-management

[7] However, this coordination is not a goal as such, but can be seen as an ambition in the long run.

[8] Many of those are based on national implementations of a voluntary, sector agnostic TIBER-EU framework that allow mutual recognition and, if agreed by all relevant stakeholders, could be used as an option for a coherent cyber resilience testing framework for significant market participant and infrastructures across the EU.

15. A coherent framework could also facilitate knowledge exchange at the EU level to share the lessons learned and high level relevant entity specific findings of tests performed at all levels, even those performed by the regulated entities themselves without authority's involvement. To avoid information leaks, no relevant entity-specific information would be exchanged in relation to the testing exercise. Taking into account potential sensitivities related to information exchange, information shared would be limited, for example, to exchanging lessons learned, best practices, and high-level aggregated findings. No database containing relevant entity-specific data would be established to avoid a single point of failure. Further details on how this knowledge exchange could be facilitated, will have to be specified during the next practical implementation phase.

16. Following the analysis conducted, the ESAs, in principle, see the benefits of a coherent cyber resilience testing framework across the EU financial sector. This could help to increase financial sector resilience by increasing awareness of cyber related risks and facilitate knowledge exchange in order to develop cyber resilience capabilities.

17. However, at present there are significant differences across and within financial sectors in terms of cyber maturity. The ESAs therefore believe that it would be premature to pursue a specific cyber resilience testing framework at this stage. The ESAs consider that a multi-staged approach to building a coherent cyber resilience testing framework would be the most appropriate.

18. The ESAs acknowledge the need to ensure proportionate application of cyber resilience testing requirements. However, it is important to emphasise that cyber resilience measures should be proportionate not only to the type, size or financial profile of a relevant entity, but also to the risks they are exposed to and the systems and services that need to be protected and maintained. For example, the presence of online services may require certain security standards to be in place regardless of the size of the relevant entity, therefore the main focus should be on service criticality and systemic importance of a relevant entity, but not on its size. Some small relevant entities might be so critical that they would be deemed subject to the TLPT testing. Hence, at times criticality might have to prevail over proportionality.

19. This advice sets out immediate short-term objectives and suggests a long-term aim, without providing technical details of practical implementation steps. More work is needed by the ESAs together with other authorities and experts to address specific practical and policy implementation questions. Such questions could include, for example: i) what should be the roles of relevant authorities and experts involved (e.g. Competent Authorities (CAs), Financial Stability Authorities, ESAs, ECB, ENISA, ESRB); ii) what should be the scope and definition of 'significant' market participants and infrastructures?; iii) are there any legal obstacles for conducting TLPT tests, e.g. to monitor employees or attempt to penetrate IT systems?; iv) legal liability aspects; v) the possibility of establishing a certification regime for testing providers and / or threat intelligence providers; vi) agreement on what specific information could be exchanged with relevant stakeholders to facilitate knowledge and skills development; vii) any potential implementation issues for cross-border relevant entities.

20. The ESAs note that a number of complex and technical design choices need to be made when implementing a coherent testing framework (e.g. the roles and responsibilities of the involved authorities, the scope of the framework, use it from financial stability or prudential supervision perspective, etc.). These detailed implementation issues are beyond the scope of the Commission's request in the FinTech Action Plan, which instead focuses on analysis of costs and benefits. Consequently, this joint Advice does not discuss such matters further.

Specific comments / proposals

21. In line with the Commission's request to provide advice on a coherent cyber resilience testing framework for significant market participants and infrastructures, the ESAs propose the following short and long term objectives:

(i) In the short term:

- that the ESAs, CAs and regulated entities focus on achieving a cyber-resilience baseline across the sectors in proportion to the needs and characteristics of relevant entities.
  In comparison with the banking sector, the insurance sector currently has less detailed regulatory requirements in the field of cyber security. In addition, the insurance sector is less homogenous size wise. Hence the cyber security maturity within the insurance sector is very diverse, with many of the main players having a higher maturity level. Therefore EIOPA will, before long, promote pilot discussions on cyber resilience testing in the colleges of supervisors of the more cyber mature insurance groups. Securities markets also involve a range of different entities, which may have differing security needs and encounter different levels of cybersecurity risk. ESMA has undertaken detailed work such as holding supervisory questionnaire exercises to identify and mitigate, on a consistent basis, cybersecurity risks facing Central Counterparties, Trade Repositories and Credit Ratings Agencies. The EBA has already developed (draft) Guidelines on ICT and security risk management for relevant entities under its remit, which set out requirement for ICT security testing, including cyber security testing. The ESAs consider that supervisory convergence initiatives such as the aforementioned guidelines will support, guide and steer regulated entities in the process of gaining cyber maturity.

- that the Commission considers facilitating the establishment by the ESAs and other relevant authorities and experts (e.g. CAs, Financial Stability Authorities, ENISA, ECB, ESRB or others) of an EU wide coherent cyber-resilience testing framework, on a voluntary basis, focusing on TLPT by taking into account existing initiatives. The ESAs believe that this issue should be examined without a preference as to the specific testing framework at this stage.

  When establishing a coherent cyber-resilience testing framework it is important not to duplicate any existing frameworks, but to focus on practical implementation aspects. It is also important that proportionality and a risk based approach are applied, and that the exercises take into account the specific cyber risk profile of the relevant entities tested. Such a framework might facilitate high-level knowledge exchange from voluntary exercises run on selected relevant entities, taking confidentiality and legal

concerns into account.

(ii) In the long term, when the necessary coherent cyber resilience testing framework is agreed, specific practical and policy implementation questions are addressed, and a sufficient cyber 'maturity level'[9] is developed across identified relevant entities, that the Commission considers the possibility for cyber resilience testing exercises to be coordinated by the ESAs and / or other relevant authorities and managed by involved authorities for the identified most systemic, critical and significant relevant entities.

Under this proposal, the ESAs, together with other relevant authorities and experts, would define principles for the expected assurance levels and the accepted sources of assurance, taking into account the particularities of each sector. This would be an important step towards building resilience and strengthening financial stability of the whole EU financial sector.

Ensuring a clear mandate

22. Against this backdrop, the ESAs advise the Commission, in order to facilitate the implementation of the above proposals:

(i) that an explicit legal basis is set out for the development and implementation of a coherent cyber resilience testing framework across the sectors under the remit of all three ESAs in the EU. This would constitute the starting point for the ESAs and other relevant authorities and experts (e.g. CAs, Financial Stability Authorities, ENISA, ECB, ESRB or others) to develop and implement a proportionate coherent cyber resilience testing framework for significant market participants and infrastructures within the whole EU financial sector; and

(ii) that the ESAs together with other relevant authorities are given an explicit mandate to develop sector-specific guidance on specific practical and policy implementation questions how a coherent cyber resilience testing framework should be implemented.

23. The detailed analysis of the points made above are set out in the appended report.

This opinion will be published on the ESAs websites.

[9] 'Cyber maturity', for example, could be defined in line with the Article 52 of the Proposal for a Regulation of the European Parliament and of the Council on ENISA, the 'EU Cybersecurity Agency', and repealing Regulation (EU) 526/2013, and on Information and Communication Technology cybersecurity certification (''Cybersecurity Act'').

Annex

Joint ESAs report on the costs and benefits of developing a coherent cyber resilience testing framework for significant market participants and infrastructures within the whole EU financial sector

Contents

1. What is cyber resilience

1.1 Definitions

1. The FSB Cyber Lexicon[10] defines 'cyber resilience' as 'the ability of an organisation to continue to carry out its mission by anticipating and adapting to cyber threats and other relevant changes in the environment and by withstanding, containing and rapidly recovering from *cyber incidents*'.

2. In addition, a 'cyber incident' is 'a *cyber event* that:
   i) jeopardizes the *cyber security* of an *information system* or the information the system processes, stores or transmits; or
   ii) violates the security policies, security procedures or acceptable use policies,
   whether resulting from malicious activity or not'.

3. In order to be cyber resilient, a relevant entity needs to have adequate 'cybersecurity' arrangements. The FSB Cyber Lexicon defines cybersecurity as the 'preservation of *confidentiality*, *integrity* and *availability* of information and/or *information systems* through the cyber medium. In addition, other properties, such as *authenticity*, *accountability*, *non-repudiation* and *reliability* can also be involved'. Cybersecurity requires security of an entity's people, processes and technology, as well as its customers and any third parties with which it interacts.

4. Based on the FSB definitions, the ESAs understand cyber resilience as protecting against malicious activities from any threat actor (internal or external), and it also includes ensuring that accidental breaches of security measures – like, for example, exposing confidential bank account holder information to the public – are avoided. It also includes the more widely known cyber threats[11] including: DDoS attacks, non-card payment fraud, CEO fraud and advanced persistent threats.

1.2 Threat led penetration testing

5. According to the FSB Cyber Lexicon, Threat-Led Penetration Testing (TLPT), also known as 'Red Team Testing' is 'a controlled attempt to compromise the cyber resilience of an entity by simulating the tactics, techniques and procedures of real-life threat actors. It is based on targeted threat intelligence and focuses on an entity's people, processes and technology, with minimal foreknowledge and impact on operations.'[12]

6. TLPT is immensely effective with respect to raising awareness on cyber resilience at a relevant

[10] FSB Cyber Lexicon, 12 November 2018. Access: http://www.fsb.org/2018/11/cyber-lexicon/. Note that definitions of terms *italic* are further explained.

[11] ENISA Threat Landscape Report 2018: https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2018

[12] FSB Cyber Lexicon, 12 November 2018

entity's board level. This is because TLPT often includes 'capture the flag' concepts that define an entity's individual most valuable assets. If the security of these assets can be compromised through TLPT, the possible consequences of not being sufficiently cyber resilient are made very visible and particular to relevant entities' senior management and board.

7. Nevertheless, in order to maximise the value of TLPT, a relevant entity needs to consider the following:
   i) A TLPT is one of the tools in a broader toolkit which organisations can use if they wish to achieve cyber-resilience. Crisis management exercises, DDoS testing and compliance regarding the rules set out by regulators regarding cyber fundamentals (e.g. in the draft EBA Guidelines on ICT and security risk management) also need to be met.
   ii) Successful TLPT exercises require a high level of threat intelligence and realistic scenarios accompanied by defined objectives;
   iii) TLPT require substantial time and resources, thus a proportionate approach in implementation needs to be considered. However in practice, most of the resources are paid for by the entity. They pay for procuring the threat intelligence and red team providers, and the white team, coordinating all test activity. The authority needs to setup a team to oversee the tests, but this can be scaled up based on the amount of entities tested;
   iv) TLPT is an advanced security-testing tool meant for mature organisations; organisations should first address their known vulnerabilities and weaknesses before engaging in a TLPT, otherwise TLPT only confirms what is already known and the appropriate maturity level for such a test might not be accomplished yet;
   v) TLPT cannot be deemed sufficient if done in isolation, and should not replace other assurance approaches and processes.

8. A TLPT framework should use threat intelligence-based scenarios which mimic real-life cyber adversaries. This is important to gain a detailed view of the specific relevant entity's key threats and deliver controlled, bespoke, intelligence-led red team tests of relevant entity's critical live production systems. Such tests aim to emulate the tactics, techniques and procedures (TTPs) of real-life threat actors who are perceived as posing a genuine threat to a relevant entity and deliver a realistic simulation of potential attacks against its critical functions and underlying systems. An intelligence-led red team test involves the use of a variety of techniques, people with high skills and expertise, robust processes and sufficient technology.

9. An important element of the TLPT tests is the replay phase, where tested relevant entities can learn from the test by letting the blue team, who defends the entity, and the red team provider, who attacks the entity, go through the steps taken by both parties in the test. This will indicate what actions were taken by the 'attacker' and what alerts or actions this triggered on the defending side. This allows the relevant entity to directly learn from the test and improve its protection, detection and response capability.

10. A TLPT testing framework should address the necessity that the tests are carried out by

independent testers (red team)[13] with sufficient knowledge, skills and expertise, and include tests adequate to reach the set goals. The tools and techniques used have to be appropriate for the test.

11. Given the inherent risks involved in such tests against live production systems (confidentiality, risk of disrupting operations of a relevant entity, third party liability, etc.), a strong risk management is required throughout the duration of the tests and thereafter. The steering team of the institute (white-team) has to be notified of the planned actions.

1.3 What is a coherent cyber resilience testing framework?

12. For the purposes of the subsequent analysis, the ESAs understand that a coherent cyber resilience testing framework is a coordinated threat led penetration testing framework in the EU. This understanding takes into account that the baseline measures for cyber resilience are set out in sector-specific guidance, which elaborate security testing requirements (e.g. in the draft EBA Guidelines on ICT and security risk management), and that a coherent framework for TLPT across the EU, including a cross-border coordination, is not yet agreed on and implemented by ESAs and other relevant authorities and experts (e.g. CAs, Financial Stability Authorities, ECB, ENISA, ESRB).

13. A coherent cyber resilience testing framework should adhere to a common set of principles, in order to facilitate mutual recognition of testing methodologies and their results.

14. As a TLPT framework is the most advanced tool for cyber resilience testing, it should be understood that to be 'coherent' it does not need to test for overall cyber resilience, but can only test certain aspects of it.

15. The joint ESAs Advice does not cover all cyber resilience aspects. For example, crisis management is not covered. Indeed, the Advice covers only one specific element of all security testing tools, namely threat led penetration testing. There are a number of tests, e.g. disaster recovery testing, that are conducted by relevant entities without the direct involvement of authorities. As a result, this advice cannot and does not cover the complete universe of security and resilience testing.

16. In addition, this Advice does not address practical implementation questions that will have to be specified by the ESAs together with other relevant authorities and experts (e.g. CAs, Financial Stability Authorities, ECB, ENISA, ESRB) to develop sector-specific guidance on how a coherent cyber resilience testing framework should be implemented. A few open questions (amongst others) relate to:

    - Scope of application and definition of a 'significant' relevant entities or infrastructures for the purposes of cyber resilience;

[13] Regarding the insurance sector, consideration should be given to IAIS 'Application paper on supervision of insurer Cybersecurity' which states that a 'red team' may consist of insurance undertakings' own employees and / or outside experts who are in either case independent of the function being tested. In Solvency II, in relation to key functions, it is understood that own employees could be operationally independent.

- Determination of level of cyber maturity for entities to be subject to TLPT tests;
- Potential certification requirements for external testing providers and / or threat intelligence providers to facilitate mutual reliance;
- Roles of authorities and experts involved (CAs, financial stability authorities, ESAs, ENISA, ECB, ESRB and/or others) including the scale and scope of coordination and implementation activities;
- Voluntary or mandatory nature of the TLPT tests;
- Determination on how the results of tests could be used (e.g. as a catalyst to raise overall cyber resilience in the financial sector and/or as a tool for prudential supervision);
- Any legal aspects of conducting TLPT tests, such as third party liability risk or confidentiality requirements.

2. Overview of current landscape of cyber resilience assurance

17. A number of national, EU level and global initiatives recognise the need for ICT security and focus on building cyber resilience.

National level

18. To map the resilience testing practices in the EU, in September 2017 the EBA conducted a survey on supervisory practices around cybersecurity in the EU financial sector. It identified that there were many differences in the process of testing of regulated entities' vulnerability and resilience to cyber risk (such as through penetration testing or other tests) and the cross-border cooperation with regards to such testing. The survey revealed that only a few authorities organised penetration testing or gave guidance on such testing to relevant entities. The majority of respondents indicated not having pen-tested regulated entities' vulnerability and resilience to cyber risks.

19. In May 2018 the ECB published a framework for threat intelligence based ethical red teaming (TIBER–EU), which is a common framework that delivers a controlled, bespoke, intelligence-led red team test of entities' critical live production systems. It is a voluntary framework that is sector agnostic. The TIBER-EU framework is designed to be adopted by relevant authorities in any jurisdiction, on a voluntary basis and from a variety of perspectives, namely as a supervisory or oversight tool, for financial stability purposes, or as a catalyst in collaboration with market participants. The relevant authorities consider which entities could be invited to participate in the programme.

20. The examples of national cyber resilience testing frameworks include CBEST[14] in the UK, and TIBER-NL[15] in the Netherlands (a TIBER-EU implementation). TIBER-NL (2016) has formed the basis for the development of the said TIBER-EU framework and has further developed the previously existing CBEST framework dating 2014. Currently in the EU the TIBER-EU framework is (in the process of) being implemented in the Netherlands, Denmark[16], Belgium[17], Ireland and the ECB Eurosystem (in its oversight capacity). Other jurisdictions are expected to follow soon.

Box. A. What is the TIBER-EU framework?

TIBER-EU, which stands for Threat Intelligence-based Ethical Red Teaming, is the first EU-wide framework for controlled and bespoke red team tests against cyber-attacks that can be used by any national or supranational jurisdiction to have their most systemic entities tested.

The TIBER-EU framework facilitates a harmonised European approach towards intelligence-based tests that mimic the tactics, techniques and procedures of real attackers who can be a genuine threat by using threat intelligence. TIBER-EU based tests are tailor made to simulate a cyber-attack on an entity's live critical functions and underlying systems, such as its people, processes and technologies. This will provide the tested entity with insight into its strengths and weaknesses and will enable the entity to learn and evolve to a higher level of cyber maturity. It is not a pass or fail test.

The TIBER-EU framework has been designed for (supra)national authorities and entities that form the core financial infrastructure, including entities with cross-border activities which fall within the regulatory remit of several authorities. The framework can be used for any type of financial sector entity, as well as entities in other vital sectors. By using optional and mandatory requirements the framework can be adapted to the specific jurisdiction while still being in line with the TIBER-EU Framework that facilitates mutual recognition which lowers the burden on both authorities and entities.

TIBER-EU was jointly developed by the ECB and ESCB national central banks, approved by the ECB's Governing Council and published in May 2018. It takes into account the lessons learned from earlier frameworks like the UK's CBEST and TIBER-NL.

21. One practical implementation of the TIBER-EU framework, a TIBER-NL, demonstrates the interplay between the financial stability authority and the supervisory authority.

Box B. TIBER-NL – a framework set up from a financial stability perspective

TIBER-NL is set up from a financial stability perspective and ran by the central bank (catalyst role). The participants participate on a voluntary basis and the supervisor/overseer is involved in validating the TIBER scoping document (showing the flag systems and compromise actions), and is informed after the test has ended and the remediation plan has been written. A summary of the report is shared while the full report can only be reviewed on the relevant entities' premises. The TIBER-NL Team at the central bank is ring-

[14] https://www.bankofengland.co.uk/financial-stability/financial-sector-continuity

[15] https://www.dnb.nl/en/news/news-and-archive/nieuws-2017/dnb365801.jsp

[16] http://www.nationalbanken.dk/en/financialstability/Operational/Pages/TIBER-DK-and-implementation-guide.aspx

[17] https://www.nbb.be/en/payments-and-securities/tiber-be-framework

fenced from the colleagues from oversight and supervision and the planning of the tests is only known in the TIBER team. Importantly, as a feedback loop generalised learnings from the tests may be incorporated in the existing compliance controls. Spear phishing for example is a widely successful attack method. Having a discussion regarding taken and planned mitigating measures and how these are tested may prove helpful. Subject oriented discussions like this will form a starting point how a relevant entity should implements its security measures effectively and how risk based compliance controls can be better formulated.

The role of supervisor and oversight colleagues is hard to overstate. The TIBER team of the central bank only helps the relevant entity deliver a controlled test that the relevant entity learns from. Whether the actual learning takes place is to be monitored by the supervisory side of the central bank as the TIBER teams role stops after finishing the test.

EU level

22. On 6 July 2016, in the aim of dealing with Member States shared issue of cybercrime, the European Union adopted the Network and Information Security (NIS) Directive (Directive 2016/1148/EU). It establishes specific measures for the implementation of a common high level of security of network and information systems across the Union. It also establishes a mechanism to support and facilitate strategic cooperation and the exchange of best practices with a view to achieving a high common level of security of network and information systems in the EU. This is the first initiative taken to face the challenges of cyber security, thus revolutionising the European resilience and cooperation system. However, the NIS directive is not fully harmonised, is subject to national implementation and only applies to designated operators of essential services. The NIS Directive covers cyber resilience at three levels:

    - *at institution level*, the NIS Directive introduces requirements for security measures and reporting of incidents of significant impact;
    - *at a national level* the NIS Directive foresees national cybersecurity strategies and the establishment of national competent authorities and CSIRTs for all sectors (including the financial sector: credit institutions, central counterparties and trading venues, etc.); and
    - *at an EU level* the NIS Directive introduces the Cooperation Group and the CSIRTs Network to facilitate collaboration and information exchange between the Member States.

23. At EU level, the EBA published *Guidelines on ICT Risk Assessment under the SREP* (EBA GL 2017/05) in 2017, which complement the *EBA Guidelines on SREP and stress-testing* (EBA GL 2018/03). They promote common procedures and methodologies for competent authorities to assess an relevant entity's ICT risk, bringing to the fore the need for supervisors to have a specific understanding of ICT risk. Furthermore, in December 2018, in response to the European Commission's *FinTech Action Plan* request, the EBA published draft *Guidelines on ICT and security risk management* (EBA CP 2018/15)[18]. The guidelines are addressed to all relevant entities and provide guidance regarding measures to mitigate ICT risks, including security risks that the relevant entities are exposed to. They elaborate on an important part

[18] To be finalised in Q3 2019.

of ICT risk mitigation – Information security, and require the establishment of strong security measures, the testing of these measures and awareness and training within the organisation and with relevant third parties.

24. Finally, in October 2018 the European Council called for measures to build strong cybersecurity in the European Union as part of the Reform of cybersecurity in Europe[19]. The European Commission and the High Representative proposed to reinforce the EU's resilience, deterrence and response[20] by proposing a series of measures such as reinforcing the European Union Cybersecurity Agency built on the Agency for Network and Information Security (ENISA) and the creation of an EU-wide cybersecurity certification scheme that will increase the cybersecurity of products and services in the digital world. Moreover, the Commission is working on a new Directive on the combatting of fraud and counterfeiting of non-cash means of payment to provide for a more efficient criminal law response to cybercrime.

International level

25. At international level, in 2017, the FSB conducted a stocktake on cybersecurity regulatory and supervisory practices that highlighted that two thirds of reported regulatory schemes took a targeted approach to cybersecurity and/or information technology risk and that most regulatory schemes covered some element of testing.

26. In June 2018, IAIS (International Association of Insurance Supervisors) has published draft '*Application Paper on Supervision of Insurer Cybersecurity*'[21].

27. In October 2018, the G7 Cyber expert group published its *Fundamental Elements on Threat led penetration testing*[22] setting out the main components for such a testing framework.

28. In December 2018, the Basel Committee on Banking Supervision published the report '*Cyber-resilience: Range of practices*'[23]. It identifies, describes and compares the range of observed bank, regulatory and supervisory cyber-resilience practices across jurisdictions.

[19] European Council of the European Union, Reform of cybersecurity in Europe, https://www.consilium.europa.eu/en/policies/cyber-security/

[20] European Commission, *Cybersecurity Factsheet*, https://www.consilium.europa.eu/media/21480/cybersecurityfactsheet.pdf

[21] IAIS, June 2018, *Application Paper on Supervision of Insurer Cybersecurity,* https://www.iaisweb.org/page/consultations/closed-consultations/2018/application-paper-on-cyber-security//file/75304/draft-application-paper-on-supervision-of-insurer-cybersecurity

[22] G7 Fundamental Elements on Threat Led penetration testing: https://www.fin.gc.ca/activty/G7/pdf/G7-penetration-testing-tests-penetration-eng.pdf

[23] BCBS, December 2018, *Cyber Resilience: Range of practices*, https://www.bis.org/bcbs/publ/d454.pdf

3. Benefits, risks and costs of using a coherent cyber resilience testing framework

29. This section provides an analysis based on available evidence on potential benefits, risks and costs of a coherent cyber resilience testing framework for significant market participants in the EU. The analysis focuses on the comparison of establishing a coherent cyber resilience testing framework for significant market participants in the EU versus of an alternative option where no harmonisation in cyber resilience testing is achieved across the EU.

30. Although the implementation and actual conduct of threat-led penetration tests have pros and cons on their own, the joint ESAs Advice goes beyond these and instead examines the case for a coherent framework in the EU.

31. The analysis that follows is based on experience of authorities conducting such programmes at national level, and aggregated feedback received from relevant entities being subject to such programmes. The development of this advice benefited from the liaison with the European Banking Federation (EBF) and the Association for Financial Markets in Europe (AFME) to obtain high-level industry views.

3.1 Expected benefits

32. Main expected benefits of a coherent threat-led penetration testing framework within the EU for significant market participants can be summarised as follows:

i. **A coherent threat-led penetration framework may lead to tests that will raise the awareness of cyber security related issues to the Board level, leading to an overall increase of cyber resilience of the financial sector at EU level**. A properly designed test that targets or identifies unknown weaknesses may make those vulnerabilities specific to each particular relevant entity and contribute to its preparedness. In addition, a coherent TLPT framework may unveil common weaknesses with potential systemic impact between the EU jurisdictions.

ii. **A coherent threat-led penetration framework may contribute to a closer cooperation and coordination of information and knowledge sharing across the EU financial sector.** Given the systemic nature of the cyber risk and the interconnectedness of EU relevant entities, the development of a coherent testing framework may be valuable in enhancing the sharing of resources, threat information, high level results and experiences between CAs, threat intelligence and penetration testing providers, and authorities involved in the coordination of the exercises and analysing the shared information. One of the main benefits of conducting TLPT tests is bringing all stakeholders together and collaborating

in building the cyber resilience, instead of simply pointing to the shortcomings identified during the tests.

iii. **A coherent framework could facilitate knowledge exchange at the EU level to gather and analyse high level findings of tests performed at all levels, even those performed by the relevant entities themselves without an authority's involvement**[24]. Cyber security should not be treated as a competitive advantage, but rather a baseline that is proportionate to the needs of different relevant entities. To facilitate this, aggregate level information on key lessons learned how to conduct TLPT tests, generic findings on key vulnerability trends identified, common remediation measures, and best practices could be exchanged among the stakeholders. The exact technical details and detailed technical descriptions of vulnerabilities would not be shared. The findings and the detailed technical reports should remain only at the relevant entities. There should not be a single database with all the vulnerabilities identified. However, the relevant entities could further benefit from an involvement in private sector information sharing and cooperation initiatives, to exchange relevant information on a timely basis.

iv. **A coherent threat-led penetration framework may promote the mutual recognition of cyber-resilience tests.** Taking into consideration that several EU countries are currently working on the implementation of cyber-resilience testing frameworks (many of those are national implementations of the TIBER-EU framework already allowing mutual recognition), the use of frameworks built on a common set of rules for cyber-resilience testing should promote the mutual acceptance of different tests across the EU and help to avoid the duplication of test and reduce costs and efforts for both relevant entities and authorities. This would facilitate cross-border supervisory or oversight equivalence discussions allowing authorities to rely on each other's assessments, leading to greater supervisory convergence.

v. **Reduced risk of duplicative or overlapping tests could save costs of any potentially unnecessary tests**. A reduced risk of multiple overlapping threat-led penetration tests would reduce the administrative and financial burden for significant market participants subject to TLPT tests. Besides the cost-efficiency, a coherent framework recognised by all EU authorities could avoid unnecessary duplication of testing efforts (by relevant entities and/or supervisors) and the risk that multiple local practices that would be otherwise used do not live up to a best practice.

vi. **A coherent TLPT framework should enable cross-sectoral convergence.** A common cyber-resilience testing framework for significant market participants may provide regulated entities, CAs and ESAs with organisational efficiencies to transfer the knowledge between all three ESAs sectors, and create the protocol for cross-authority cross-border collaboration. In particular, a coherent cyber resilience-testing framework may benefit the competent authorities when supervising relevant entities that belong to various sectors of financial services, by leveraging experts' knowledge of uniform methodology

[24] 'Cooperation Group' as defined in Article 11 of NIS Directive (Directive 2016/1148) can be used as an example.

across different sectors of financial services.

vii. **A coherent EU-wide TLPT framework would facilitate the creation of a single market for external threat intelligence and test providers.** The application of a coherent framework, including a coherent requirement for tests and external test providers (e.g. in form of minimum quality requirements or certification regime) across all EU member states would help to establish a larger pool of capable external test providers, increasing the quality and reducing the price of the TLPT tests.

viii. **Overall, in the long term, a coherent framework would be beneficial to the awareness and preparedness of significant market participants and infrastructures to cyber related risk, leading to an overall increase of cyber resilience of the financial sector at EU level.** Reduced financial stability risks would enable better consumer protection and maintaining trust in the financial sector to provide essential services to businesses and retail customers.

Box C. Lessons learned from the TIBER-NL exercise

TIBER-NL is a threat led operational resilience testing program and aims to test the capability of actual advanced attackers by mimicking their attack methods. People, processes, facilities and systems are being included in the test on the live key production systems as well as third parties.

The added value of these tests as experienced by the (approximately 30) Dutch financial institutions (FIs) undergoing the test is most easily expressed in their voluntary financing of a third of the costs of the central team running the program at the national central bank (DNB) and their agreement (mid 2018) to extent the TIBER-NL program for another 3 year period. They help by financing the senior test managers and collectively buy sector specific intelligence.

FIs emphasise that the main added value lies in: i) the **trusted community** the TIBER-NL tests forms, ii) the governmental intelligence agencies **validating** the sector intelligence, iii) the many **learnings** the test offers the tested FI, iv) the sharing of **best practices** resulting from the tests, v) the collective capability to identify and **improve concentration** risks, vi) the costs that are being avoided by having their test results **recognised in multiple jurisdictions**, vii) the **collectively** buying of threat intelligence and viii) the **professional advice** given by experienced colleagues from other FIs in the trusted community. A further benefit is the board level attention the TIBER-NL tests result in, more so than internal tests.

Criticism has been expressed as well. Due to applicable strict requirements (e.g. background checks, references, experience) the highest-end security testing market is small. Notwithstanding the strict requirements, the maturity level of testing that the threat intelligence and red team providers deliver varies. It is highly dependent on personal skills of the team engaged. Testing under the TIBER-NL scheme is time and resource intensive and should not be done more than once every 2-3 years.

3.2 Potential risks

33. A lack of a coherently implemented cyber resilience testing framework for significant market participants and infrastructures risks creating a fragmented approach in the EU to test cyber resilience of relevant entities. This would undermine the main purpose of a single rulebook and the convergence of supervisory and regulatory approaches for cross-border relevant entities. In addition, possible duplication of TLPT exercises could significantly increase the financial and regulatory compliance burden for the affected relevant entities.

34. The ESAs therefore consider that the implementation of a coherent cyber resilience testing framework needs to be carefully designed, in order to avoid any possible negative implications, for example:

- **Degree of flexibility** – in a coherent framework there will be a need to tailor the tests to a particular relevant entity and adjust them the specific local market conditions. The approach does not have to be identical in different situations, but it has to be consistent. Jurisdictions should be able to adopt a framework, with degrees of flexibility on implementation within known and accepted parameters.
- **Adherence to cyber maturity level** – a coherent cyber resilience-testing framework should not disregard the different maturity in cyber security within and across various financial sectors across three ESAs.
- **Requirements for threat intelligence and test providers** – the granularity of a coherent cyber resilience-testing framework must be carefully set: on the one hand, it is not desirable to remove service providers from the market who do possess the technical expertise, but might not be able to meet requirements if they are too restrictive; a too lenient framework might, on the other hand, defeats its own purpose. The risk of concentration of expertise within few companies, able to perform penetration testing in line with the framework, should be assessed and managed.
- **Level of involvement of public authorities** – finally, it is important to determine the level of involvement of the different authorities, as a coherent cyber resilience testing framework could pose an additional challenge to them in terms of number of staff resources and the skillset required.

35. Moreover, a coherent cyber resilience testing framework would entail a number of TLPT tests being conducted on identified significant relevant entities. Although these tests aim to increase cyber resilience and are designed with a number of safeguards in place to ensure safe execution, there are certain risks associated with conducting a TLPT for cyber resilience purposes. These would also be relevant if a non-coherent framework is being used. Some of the risks are outlined below:

i. **It should be understood that a coherent threat-led penetration framework does not address all cyber resilience challenges and that it needs to be applied together with other tools.** A coherent cyber-resilience framework will not cover all vulnerabilities and will not achieve comparability across the financial sector. However, TLPT should contribute to building cyber resilience. Relevant entities are very different in their underlying technologies, services offered, and operating models, therefore the different

scopes of the tests could make comparability across the tests difficult to achieve. In addition, the heterogeneous level of expertise within relevant entities and CAs could hinder the implementation of a coherent framework or may result in different implementations.

ii. **A TLPT test reflects weaknesses in only one point in time.** Because of the rapidly evolving nature of ICT, it is possible that there might be an attack vector that was not covered during the test because it was unknown. As a result, it can only be concluded that an entity was secure at this specific point in time.

iii. **A coherent threat-led penetration framework may result in a potential information leak about serious vulnerabilities in relevant entities.** Following the sharing of high level test results, an increased amount of stakeholders will increase awareness of the general vulnerabilities of relevant entities that participated in the tests. To limit this risk, sensitive relevant entity-specific information will not be shared. Reports with the detailed technical description of the vulnerabilities should remain in the relevant entities.

iv. **A coherent threat-led penetration framework may reveal a potential shortage in skilled resources able to perform cyber-resilience tests.** If a significant number of relevant entities in Europe are requested to test themselves simultaneously, it may happen that there are not enough sufficient skilled and reliable testing providers available to perform the cyber-resilience tests. In addition, a lack of sufficient competencies may be identified in public authorities (such as supervisors and coordinating EU authorities), where reliance on the use of external specialised resources could bring confidentiality concerns.

v. **A TLPT test performed on live production systems could cause system outages.** The framework needs to ensure strict procurement guidelines for test providers, ensure that there is enough internal knowledge of the systems that are being tested, and there is a continuous involvement of the team with knowledge of these type of tests that could signal to stop if there is too much risk taken.

3.3 Costs of using a threat-led penetration testing framework (early evidence)

36. At this stage, the costs of implementing of a coherent cyber resilience testing framework for significant market participants and infrastructures in the EU can only be approximated, as actual implementation of a coherent framework requires a number of complex design choices that are out of perimeter of this joint ESAs Advice.

37. On the one hand, there will be one-off public sector costs to establish a governance mechanism for a coherent cyber resilience testing framework involving ESAs and other relevant authorities and experts (e.g. CAs, Financial Stability Authorities, ENISA, ECB, ESRB), and associated continuous expenses to support the maintenance and regular update of the framework, including the facilitation of knowledge exchange within the public authorities

and providing feedback to private sector. On the other hand, significant private sector cost reduction is expected due to avoidance of otherwise overlapping requirement to conduct national tests.

38. The ESAs suggest that more detailed cost and benefit analysis is conducted in the next phase when specific implementation aspects of a coherent cyber resilience testing framework for significant market participants are considered.

39. The following section provides some early evidence from the TLPT tests conducted by a few relevant entities in the banking sector in a few EU Member States. Other parts of the financial sector can have different characteristics. The findings are based on a survey that the EBA conducted in January-February 2019 with selected credit institutions and banking federations on the early experiences of TLPT tests. In total, 10 responses were received, and so the results cannot be considered as being representative. However, they provide a valuable illustration of the potential magnitude of costs associated with the TLPT.

For significant market participants and market infrastructures

40. Cyber resilience testing is a complex exercise that require relevant entity's internal staff allocation and monetary expense to obtain threat intelligence and contract external test provider. The results of a non-representative sample of relevant entities (based on the responses from 10 respondents, 4 of which participated in TLPT testing) revealed that a lack of harmonised framework in the EU could lead to a number of additional potentially duplicated tests. Based on their organisational structure in two cases relevant entities could be subject to up to two TLPTs per year, and in one case they could be subject to three TLPTs per year. For relevant entities with a global presence outside the EU, additionally 1 to 3 TLPTs might be required. As result, the potential cost-efficiency might be significant.

41. In terms of internal ICT staff needs, evidence from seven responses received suggest that internal resources and costs associated with TLPT run by external providers are estimated at between 1 and 50 full time equivalents (FTEs) for each TLPT. The proportion of internal staff for such exercise in relation to the total ICT staff in the respective entities range between 0.1% and 5%. The overall costs of TLPT exercises in three cases, where it was possible to assess them separately (i.e. TLPT costs not being integrated in the security budget or considered to be a business test), were estimated in a range between 0.1% and 0.3% of the total ICT budget. However, actual resources associated with TLPT testing might be higher, if indirectly related staff involvement (e.g. staff from risk, legal, business lines, etc.) is taken into account.

42. The costs of hiring the external threat intelligence and test providers vary across individual relevant entities and different jurisdictions where the tests take place. Costs depend on the scope of the engagement, target objectives and established timeframe. Sector specific intelligence (generic intelligence) can be procured centrally. For example, in case of the TIBER-NL exercises, it was purchased by the national central bank and is provided to stakeholders via a dedicated platform. The risks involved with generic data sharing is limited

as the data stored on the platform will not contain relevant entity-specific data or live vulnerabilities.

For involved public authorities

43. Based on TIBER-NL experience, to facilitate setting up the program 1-2 FTEs are expected to be necessary. Further resources needed to run a test for a number of selected relevant entities are 3 FTEs, and additional program running cost are needed to cover, e.g. training, hiring, advice, and travel needs. The intelligence analysis (when done centrally) would require a minimum additional FTE. When closely collaborating with the sector cyber threat intelligence specialists efficiency can be achieved. In the Dutch experience 3 to 4 FTEs were needed for running a test base of 15 relevant entities (6 to 7 tests per year), and 8 to 9 FTEs for running tests for 30 relevant entities (12 to 15 tests per year). The latter is build up as follows: a manager, two senior test managers, two mid-level test managers (to work in pairs on each test), a program secretary, a policy maker and one or two employees responsible for threat intelligence.

3.4 Conclusions of ESAs analysis

44. The precise costs and especially benefits of a coherent cyber resilience testing framework are difficult to quantity as they depend on the scope and scale of the TLPT exercises and the envisaged roles of the stakeholders involved.

45. Nevertheless, the analysis conducted by ESAs on the basis of i) early evidence from TLPT tests conducted by relevant entities and ii) the feedback received from CAs suggests that the value-added of a coherent cyber resilience testing framework in the EU would outweigh the cost associated with developing and running it. This holds especially if mutual reliance on tests results can be facilitated and ensured, and duplication and overlap of tests is avoided. Mutual recognition of tests would reduce the regulatory and financial burden for relevant entities that operate on a cross-border basis across the EU, while supported information sharing and mutual collaboration among the involved authorities would contribute to the enhancement of the overall cyber resilience within the EU. Building on the existing contacts within the trusted community would help relevant entities in an actual crisis situation.

4. Conclusions

46. The ESAs believe that cooperation between the relevant stakeholders based on a coherent cyber resilience testing framework for significant market participants can support good and consistent risk management across the financial sector in relation to cyber security. This should in turn help promote effective and secure delivery of financial services across the EU while supporting consumer and market trust.

47. However, the details of the application of a coherent cyber resilience testing framework may vary both between and within sectors, depending on i) the cyber security maturity level of the market participants, ii) the systemic importance of the specific sectors, iii) criticality of the service provided by the market participants and infrastructures, and/or iv) national cybersecurity strategies for certain critical market participants and infrastructures.

48. The ESAs recognise that cyber resilience testing covers a wide variety of tools and actions, ranging from a basic level of security testing to threat intelligence led penetration testing (TLPT).

49. TLPT is one tool in a broader toolkit, which relevant entities should consider if they wish to achieve cyber-resilience. However, TLPT is insufficient alone to determine the complete cyber resilience stance of significant market participants and infrastructures within the EU financial sector.

50. The ESAs agree with the opinion expressed by the European Commission that '*Assessing cyber resilience of significant financial market players across the EU financial sector has the potential to efficiently and effectively identify vulnerabilities of the stability and integrity of the entire EU financial system*.' The ESAs see testing as a tool to assess the capability of a relevant entity to face actual threats, and agree that in case of significant relevant entities, a coherent TLPT framework is worthwhile. More so, because such a framework stimulates sharing of best practices and makes it possible to raise the sector cyber resilience and contribute to overall financial stability.

51. Following the analysis conducted, the ESAs, in principle, see the benefits of a coherent cyber resilience testing framework across the EU financial sector.

52. TLPT may be extended to relevant entities with mature cybersecurity in place, in particular to the selected significant relevant entities. Nevertheless, all relevant entities need to focus on strengthening the 'cyber fundamentals' and will benefit from testing their capabilities on these, e.g. as outlined in the draft EBA Guidelines on ICT and security risk management.

53. Due to differences across and within financial sectors in terms of cyber maturity, the ESAs believe it would be premature to pursue a specific cyber resilience testing framework at this stage. The ESAs consider that a multi-staged approach to building a coherent cyber resilience testing framework would be the most appropriate.

54. In the short term the ESAs, CAs and relevant entities should focus on achieving a cyber-resilience baseline across the sectors in proportion to the needs and characteristics of individual relevant entities. In addition, the Commission should consider facilitating the establishment by the ESAs and other relevant authorities (e.g. CAs, Financial Stability Authorities, ENISA, ECB, ESRB or others) of an EU wide coherent cyber-resilience testing framework, on a voluntary basis, focusing on TLPT by taking into account existing initiatives.

55. In the long term, when the necessary coherent cyber resilience testing framework is agreed, specific practical and policy implementation questions are addressed, and a sufficient cyber 'maturity level' is developed across identified relevant entities, the Commission should consider the possibility for cyber resilience testing exercises to be coordinated by the ESAs and / or other relevant authorities and managed by involved authorities for the identified most systemic, critical and significant relevant entities.

56. In order to facilitate the implementation of the above proposals an explicit legal basis is needed for the development and implementation of a coherent cyber resilience testing framework across the sectors under the remit of all three ESAs in the EU. In addition, the ESAs together with other relevant authorities and experts (e.g. CAs, Financial Stability Authorities, ENISA, ECB, ESRB) should be given an explicit mandate to develop sector-specific guidance on how a proportionate coherent cyber resilience testing framework should be implemented.

57. More work is needed by the ESAs together with other authorities in the course of developing sector-specific guidelines to address specific practical and policy implementation questions. Associated comprehensive cost-benefit analysis should be carried out on all important implementation and policy questions, such as:

- Scope of application and definition of a 'significant' regulated entities or infrastructures for the purposes of cyber resilience;
- Determination of level of cyber maturity for entities to be subject to TLPT tests;
- Potential certification requirements for external testing providers and / or threat intelligence providers to facilitate mutual reliance;
- Roles of authorities and experts involved (e.g. CAs, Financial Stability Authorities, ENISA, ECB, ESRB, and ESAs), including the scale and scope of coordination and implementation activities;
- Voluntary or mandatory nature of the TLPT tests;
- Determination on how the results of tests could be used (e.g. as a catalyst to raise overall cyber resilience in the financial sector and/or as a tool for prudential supervision);
- Any legal aspects of conducting TLPT tests, such as third party liability risk or confidentiality requirements.