Conseil de
l'Union européenne

Bruxelles, le 16 mars 2022
(OR. fr, en)

Dossier interinstitutionnel:
2020/0266 (COD)

7092/22
ADD 1

LIMITE

EF 75
ECOFIN 213
TELECOM 101
CYBER 81
IA 24
CODEC 297

NOTE

Origine:	Secrétariat général du Conseil
Destinataire:	Comité des représentants permanents
Objet:	Règlement sur la résilience opérationnelle numérique du secteur financier et modifiant les règlements (CE) nº 1060/2009, (UE) nº 648/2012, (UE) nº 600/2014 et (UE) nº 909/2014 (DORA) - Document de travail de la Commission (Tests)

Proposal for a Regulation on Digital operational resilience for the financial sector (DORA)

Digital Operational Resilience testing

Non-paper for DORA trilogues

DISCLAIMER

This non-paper has not been adopted or endorsed by the Commission. Any views expressed therein shall not be regarded in any way as stating an official position of the Commission. The information contained within is exclusively intended for discussions with the Union co-legislators in the context of the inter-institutional trilogues on DORA.

Following the first political trilogue, the co-legislators mandated the Commission services to provide an overview of the practical aspects of the proposals on the table as regards threat-led penetration testing, and, if possible, propose workable compromises notably as regards the relationship with TIBER-EU and supervisory responsibility for testing.

1. Background

TIBER-EU stands for Threat Intelligence-Based Ethical Red-teaming, and has been developed by the European Central Bank (ECB) in 2018. TIBER-EU is a voluntary framework and since its adoption, it has been implemented or is in the process of being implemented in 13 Member States.

The main objective of TIBER-EU is to assess the protection, detection, response and recovery capabilities of financial institutions and market infrastructures against a simulated real-life cyber-attack. In order to achieve this objective, TIBER-EU foresees a set of key phases and activities, as well as some mandatory and optional requirements in the adoption and implementation process.

The advanced digital operational resilience testing in DORA is largely inspired from TIBER-EU. DORA lays down a framework for coordinated testing by significant financial entities and competent authorities in order to ensure robust digital operational resilience and facilitate the mutual recognition of advanced testing approaches while reducing the administrative burden and costs for significant financial entities holding multiple licences and/or operating in multiple jurisdictions across the Union. The accompanying impact assessment[1] highlighted that the lack of mutual recognition of testing results could subject cross-border financial entities to a range of two to five similar tests in different Member States. This would translate into additional administrative burden and costs that could range between 250.000 EUR and 2 million EUR per financial entity.

2. Overview and interaction of the core components of TIBER-EU with DORA

There are three core components of the TIBER-EU framework on which the approach of the Council and the European Parliament diverge:

1) the testing environment, i.e. on live production systems vs. the pre-production environment;
2) the type of testers, i.e. external vs. internal testers; and
3) the designation of authorities responsible for the digital operational resilience testing in each Member State, i.e. one single authority vs. several authorities.

[1] https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12090-Financial-services-improving-resilience-against-cyberattacks-new-rules-_en

Testing Environment

The TIBER-EU framework foresees tests to be performed on live production systems. This core component of the framework is mandatory in the implementation process by the Member States that decided to implement TIBER-EU.

The Commission accordingly incorporated this core component of TIBER-EU by proposing in Article 23(2) that advanced testing shall be performed on live production systems that support the critical functions and services of a financial entity.

The Council approach is similar to Commission's proposal, with some minimal amendments that do not alter the substance of the provision.

The European Parliament amendment foresee that the test shall be performed on live production systems, where possible, or on pre-production systems with the same security configuration.

Testing on live production systems enables a financial entity to get a real picture of its level of preparedness against a simulated real cyber-attack. On the contrary, testing on pre-production environment cannot fully emulate the live production environment. In addition, the pre-production environment does not have the same monitoring protocols/tools as those implemented in the live-systems. Therefore, there is a high risk that the outcome of a test performed on a pre-production environment is of a lesser relevance in assessing the effective protection, detection, response and recovery capabilities of a financial entity.

Regarding the substance of a possible compromise text, we therefore suggest to (i) rely on the Council's approach of testing on live production systems, and (ii) take elements from EP's text that clarify that the intention of a single test is not to cover all critical or important functions.

The textual proposal is provided in the Annex.

Type of testers

Another core component of TIBER-EU is the type of testers. According to the framework, tests should be conducted by external testers that are independent of the financial entity.

The Commission's proposal foresees in Article 24 that financial entities can employ either internal or external testers for advanced testing. In addition, it adds a set of requirements for the internal testers aimed to ensure they are of the highest suitability and reputability, possess technical and organisational capabilities and demonstrate specific expertise, and are certified by an accreditation body in a Member State or adhere to formal codes of conduct or ethical frameworks. While there are advantages in employing external testers (e.g. provide a fresh and independent perspective), there are also clear benefits in using internal testers that fulfil the safeguards foreseen in Article 24 (e.g. more cost effective, lower risk of breaching confidentiality, etc.).

The Council approach is aligned with the TIBER-EU framework as it allows only external testers to perform advanced testing.

The European Parliament approach is similar to Commission's proposal, as both internal and external testers are eligible to perform advanced testing. Moreover, the European Parliament's text adds some additional safeguards concerning the internal testers. More specifically, their use needs to be approved by the relevant competent authority and by the single public authority designated, and these authorities have to verify that the financial entity has dedicated sufficient resources and ensured that conflicts of interest are avoided throughout the design and execution phases of the test.

In terms of a potential compromise text, we suggest to rely on European Parliament's text that allows for both internal and external testers and foresees a set of additional safeguards for internal testers.

The textual proposal is provided in the Annex.

Single vs multiple public authorities

The TIBER-EU framework is flexible and allows the designation of a single authority or jointly by several authorities. This flexibility has been translated differently in the implementation of the framework across the Union. More specifically, in some Member States one leading authority has been designated as responsible for implementing the TIBER-EU framework (e.g. in Sweden[2], the central bank (Riksbank)), while other Member States have opted for a joint adoption by two authorities (e.g. in Luxembourg[3], the central bank (BCL) and the financial supervisory authority (CSSF)), or adoption by several authorities (e.g. in Spain[4], the central bank (BdE) jointly with the securities markets authority (CNMV) and the insurance and pension funds authority (DGSFP)).

In order to cater for divergences in how Member States organise supervision, the Commission proposal was silent on the designation of authorities responsible for threat-led penetration testing, and left it to each Member State to decide in the implementation process.

The Council text builds on Commission's approach to allow each Member State to designate the authority/authorities responsible, but introduces some flexibility by granting Member States the possibility to delegate this responsibility to a single public authority in the financial sector or to other national authority in the financial sector.

The European Parliament is more restrictive on the designation, as it imposes the designation of one single authority for threat-led penetration testing at national level.

In terms of a compromise text, we suggest to rely on Council's approach to allow for a flexible implementation, so that each Member States can designate one or more authorities depending on the national arrangements and particularities. This flexibility would seem desirable given also the broad range of firms falling under the scope of DORA and by extension, the broad range of competent authorities involved. Designating one authority in charge of testing would decouple responsibility in this area from the sectoral expertise otherwise guiding the allocation of supervisory responsibility under DORA.

[2] https://www.riksbank.se/globalassets/media/tiber/implementation-guide-tiber-se.pdf
[3] https://www.cssf.lu/wp-content/uploads/TIBER-LU_Implementation_Guide.pdf
[4] https://www.bde.es/f/webbde/INF/MenuHorizontal/Servicios/TIBER-ES/Guia_implantacion_Tiber.pdf

The textual proposal is provided in the Annex.

Annex – the four columns table with the proposed compromise text

Testing environment

Article 23(2), first subparagraph				
	Commission Proposal	**EP Mandate**	**Council Mandate**	**Compromise text**
391	2. Threat led penetration testing shall cover at least the critical functions and services of a financial entity, and shall be performed on live production systems supporting such functions. The precise scope of threat led penetration testing, based on the assessment of critical functions and services, shall be determined by financial entities and shall be validated by the competent authorities.	2. Threat led penetration testing shall cover at least the critical ***or important*** functions and services of a financial entity, and shall be performed on live production systems supporting such functions ***where possible, or on pre-production systems with the same security configuration***. The precise scope of threat led penetration testing, based on the assessment of critical ***or important*** functions and services, shall be determined by financial entities and shall be validated by the competent authorities. ***It shall not be a requirement for a single threat led penetration test to cover all critical or important functions.***	2. **The** threat led penetration testing shall cover at least the critical functions and services of a financial entity, and shall be performed on live production systems supporting such functions. The precise scope of threat led penetration testing, based on the assessment of critical functions and services, shall be determined by financial entities and shall be validated by the competent authorities.	2. **The** threat led penetration testing shall cover at least the critical ***or important*** functions and services of a financial entity, and shall be performed on live production systems supporting such functions. The precise scope of threat led penetration testing, based on the assessment of critical ***or important*** functions and services, shall be determined by financial entities and shall be validated by the competent authorities. ***It shall not be a requirement for a single threat led penetration test to cover all critical or important functions***.

Type of testers

	Article 24(1), introductory part			
	Commission Proposal	**EP Mandate**	**Council Mandate**	**Compromise text**
411	1. Financial entities shall only use testers for the deployment of threat led penetration testing, which:	1. Financial entities ***and ICT third-party service providers permitted to enter directly into contractual arrangements with an external tester in accordance with Article 23(2)*** shall only use testers for the deployment of threat led penetration testing, which:	1. Financial entities **other than financial entities referred to in Article 14a and other than microenterprises** shall only use **external** testers for the deployment of threat led penetration testing, which:	1. Financial entities ***and ICT third-party service providers permitted to enter directly into contractual arrangements with an external tester in accordance with Article 23(2)*** shall only use testers for the deployment of threat led penetration testing, which:

	Article 24(1), point (ea)			
416a		***(ea) in the case of internal testers, their use has been approved by the relevant competent authority and by the single public authority designated in accordance with Article 23(3a), and those authorities have verified that the financial entity has dedicated sufficient resources and ensured that conflicts of interest are avoided throughout the design and execution phases of the test.***		***(ea) in the case of internal testers, their use has been approved by the relevant competent authority and by the single public authority designated in accordance with Article 23(3a), and those authorities have verified that the financial entity has dedicated sufficient resources and ensured that conflicts of interest are avoided throughout the design and execution phases of the test.***

Single vs multiple public authorities

Article 23(3a), first subparagraph

	Commission Proposal	EP Mandate	Council Mandate	Compromise text
400a		***3a Member States shall designate a single public authority to be responsible for threat led penetration testing in the financial sector at national level, except for the identification of financial entities in accordance with paragraph 3, including threat led penetration testing undertaken by financial entities and by ICT third-party service providers entering directly into contractual arrangements with external testers. The designated single public authority shall be entrusted with all competences and tasks to that effect.***	**3a Member States may designate a single public authority in the financial sector responsible for threat led penetration testing related matters at national level in relation to threat led penetration testing in the financial sector and shall entrust it with all competences and tasks to that effect.**	**3a Member States may designate a single public authority in the financial sector responsible for threat led penetration testing related matters at national level in relation to threat led penetration testing in the financial sector and shall entrust it with all competences and tasks to that effect.**

Article 23(4), first subparagraph, introductory part -a				
400b			**3b. In the absence of a designation in accordance with paragraph 3a, a competent authority may delegate the exercise of some or all of the tasks referred to in Articles 23 and 24 to other national authority in the financial sector.**	**3b. In the absence of a designation in accordance with paragraph 3a, a competent authority may delegate the exercise of some or all of the tasks referred to in Articles 23 and 24 to other national authority in the financial sector.**