RegCORE Client Alert

Revisiting the ECB's 2018 framework on testing cyber-resilience and combatting digital financial crime

September 2021

ECB TIBER-EU Guidelines

Revisiting the ECB's 2018 framework on testing cyber-resilience and combatting digital financial crime

Dr. Michael Huertas
Tel.: +49 160 973 757-60
michael.huertas
@pwc.com

Contact RegCORE Team
de_regcore@pwc.com

The increasing sophistication and scope of cyberattacks on financial services firms but also against central banks and financial services regulators has brought the issue of cyber-resilience into the focus of regulators and financial stability policymakers – including the EU's proposal for a new regulation for a digital operational resilience act (**DORA**) which is expected to take operational effect from 2024[1]. In 2018, the EU established a standard framework for cyber-resilience testing that addresses a wide range of firms and their operational processes and the European Central Bank (**ECB**) published its framework for Threat Intelligence-based Ethical Red Teaming (**TIBER-EU**)[2] on 2 May 2018. Both the EU and the ECB see action on financial services firms improving their cyber-resilience as crucial. The ECB wants to want to avoid a situation where a cyber incident affecting financial infrastructures could evolve into a systemic financial crisis. Assessing whether or not this will happen hinges on identifying whether a cyber incident will escalate from the operational level to the financial level, and ultimately start damaging confidence.

The ECB's new framework is voluntary and mandatory at the same time. The overall supervisory policy outcome is to improve the capabilities of supervised financial services firms but also supervisors in dealing with cyber-threats from real-life actors (regardless of provenance) and their impact on financial services firms in general but equally in respect of the "critical economic functions" the perform and what that means in terms of their impact on the wider market. For firms covered by these EU rules, this means that they must, among other things, ensure that they have suitable service providers who must meet certain standards to be certified to perform a "TIBER-EU" test.

This Client Alert assesses the ECB's 2018 publication of the TIBER-EU framework (including the **White Team Guide**) against the backdrop in 2021 of an increasing shift by financial services firms to meet

[1] DORA incorporates the lessons that have been learned from the Eurosystem's cyber resilience strategy for financial market infrastructures. It covers – implicitly or explicitly – the Eurosystem's cyber resilience oversight expectations, the European programme to test and improve the resilience of the financial sector against sophisticated cyber-attacks (TIBER-EU), and the Cyber Information and Intelligence Sharing Initiative created by the ECRB (CIISI-EU).
[2] Available here

customers' demands for digitisation, online services, mobile applications as well as a sustained move amongst firms but their counterparts and clients towards remote and location-independent working. While finance may be changing, so too are the range of threats to operational and equally cyber-resilience. Rapidly evolving threat actors that are constantly adapting their tactics, techniques and procedures (**TTP**s) to remain ahead of financial services firms' defences.[3]

Introducing TIBER-EU

TIBER-EU makes partial use of military terminology for naming various newly introduced terms. "Red-teaming" takes its name from military antecedents and refers to the process of testing vulnerabilities along with the readiness and resilience of a test subject and the capabilities and effectiveness of its response force i.e., the Blue Team. Red Team actions are unknown and masked to the Blue Team and only a select group, i.e., the White Team[4], have access to details of the test and the "flags" i.e., objectives that the Red Team has to "capture" and using TTPs, dynamically, to achieve that goal.

The TIBER-EU framework marked the ECB's first foray into the area of cyber resilience and defining what constitutes best practice along with an "Annex" which sets out requirements that are mandatory (most are) along with those those that are optional. The ECB is acting here not only in its role as a central bank but more importantly in its financial market infrastructure and financial stability oversight capacity. Equally, while TIBER-EU follows the efforts of the ECB, acting at the head of the Banking Union's Single Supervisory Mechanism (**SSM**), it goes much further than the SSM's supervisory priorities and actions on cyber-resilience to date. In particular, the CPMI IOSCO Guidance on Cyber-Resilience for Financial Market Infrastructures, which was "operationalised" by the ECB in its 2018 Cyber Resilience Oversight Expectations (**CROE**).[5]

The TIBER-EU framework also has an important role in the on-going supervision of key financial market infrastructure providers, given the framework's overriding emphasis on "critical functions" - which firms will want to distinguish with a view to the official definition used by the framework: "... the people, processes and technologies required by the entity to deliver a core service which, if disrupted, could have a detrimental impact on financial stability, the entity's safety and soundness, the entity's customer base or the entity's market conduct."

The ECB's publication also describes itself as the roadmap for how this framework "... will be applied across the EU" and not just the Banking Union. Firms should note that these ECB measures are supplemented by specific EU-wide measures, including those advanced as part of the EU's FinTech Action Plan along with best practice expectations set by the European Supervisory Authorities (EBA, ESMA, EIOPA) as well as national level authorities in several EU Member States.

DORA together with TIBER-EU provides a unique opportunity to address the current fragmentation in financial legislation and supervisory approaches in the field of digital operational resilience, including cyber resilience.

The extent of TIBER-EU's coverage

The focus of TIBER-EU is to create a common framework for a controlled environment in which red-teaming can test the resilience of entities using the tactics, techniques and procedures (the TTP as TIBER- EU calls it) employed by actual threats. This should also enable firms to assess how their people, processes and technologies are able to protect against, detect and respond to threats and attacks.

The advantage of TIBER EU is that it is jurisdiction-independent and flexible. This is mainly due to the fact that TIBER EU is based on implementation guidelines. This makes it possible for different jurisdictions to make appropriate adaptations. It also simplifies cross-jurisdictional intelligence-led testing and cooperation, allowing flexibility for users (both market participants and stakeholders) and embedding and endorsing the use of equivalence decisions so that one supervisor can rely on the assessment of another and thus foster

[3] Financial services firms may also want to take note of the annual guidance and recommendations published in the context of Europol's Internet Organised Crime Threat Assessment (**IOCTA**). IOCTA is Europol's flagship report providing a law enforcement focused assessment of evolving threats and key developments in the area of cybercrime. IOCTA should be available here from December 2021.
[4] "TIBER-EU White Team, Guidance" available here.
[5] Available here with details of international adoption and recognition available here.

mutual recognition and sharing of results. TIBER-EU is addressed to stakeholders and policymakers shaping supervisory responses to improve cyber- resilience inasmuch as market participants that may be in-scope of "TIBER-EU testing".

As with a range of other ECB rulemaking TIBER-EU is designed to be "guidance" adopted on a voluntary basis (with mandatory parts as and when the guidance is adopted) and from a variety of perspectives by supervisory authorities, whether as a tool for oversight and/or supervision or a catalyst for improvement. This soft law approach has a number of benefits, not least politically in getting support from ECB-internal stakeholders but also those authorities in the Eurosystem in terms of how these new measures impact existing mandates of EU and national level authorities.

Who is in-scope?

TIBER-EU tests also apply to a much a wider range of financial market participants that the ECB is interested in rather than just those that are supervised by it in the SSM on a or indirect basis. Paragraph 2.1 of the TIBER-EU framework states that "entities" include:

- Payment systems
- Central securities depositories
- Central counterparty clearing houses
- Trade repositories
- Credit rating agencies
- “Stock exchanges” (note the non-MiFIR/MiFID II use of terms and exclusion of IFR/IFD investment firms)
- “Securities settlement platforms” (note the non-MiFIR/MiFID II use of terms)
- “Banks” (note the non-CRR II/CRD V use of terms)
- Insurance companies
- Asset management companies – thus both AIFMs and UCITS ManCos
- “any other service providers deemed critical for the functioning of the financial sector”

Such a broad scope makes sense because the framework itself is also broad and, in addition, there are various forums that are thematically linked to the framework, such as the Euro Cyber Resilience Board for Pan-European Financial Infrastructures (**ECRB**). It is however conceivable that TIBER-EU might need to be amended to broaden its scope to a range of firm types that are within SSM supervision as well as for TIBER-EU to support the supervisory outcomes set in DORA.

TIBER-EU tests

The testing of the firms concerned is carried out by one or more competent authorities. In the case of firms operating across borders, such tests may be conducted in one of two ways:

1. On a cross-authority collaborative testing basis "directed" by one of the relevant authorities (similar to home - host state passporting), and/or

2. On a basis of a test "managed" by one of the relevant authorities (preferably the "lead" authority)

The above options are both designed to be mutually recognised and "... to provide assurance to relevant authorities in other jurisdictions, provided the core requirements of the TIBER-EU Framework have been met."

A TIBER-EU test is accepted only if:

- It is conducted by independent third-party providers (external threat intelligence (**TI**) and red team providers (**RT**); and
- It involves all stakeholders i.e., the "testing entity, which is responsible for managing the end-to-end test and ensuring that all risk management are in place to facilitate a controlled test", the TI and RT providers who conduct the test, the authorities that oversee the test and "... ensure they are conducted in the right spirit and in accordance with the TIBER-EU Framework." - NB it is not fully clear from the initial drafting whether the "testing entity" was meant to mean the test subject or a different entity.

The fundamental idea behind why service providers need to be independent is to: "... provide a fresh and independent perspective, which may not always be feasible with internal teams that have grown

accustomed to the internal systems, people and processes. Furthermore, external providers may have more resources and up-to-date skills to deploy, which would represent additional benefits for the entity."[6]

This basic idea makes sense but is rather costly for firms. In addition to the price tag, firms must be prepared to act, even if they are not formally forced to participate. It is important for firms to select providers that meet the standards set by the ECB, which also require that "...providers are accredited and certified by a recognised body to carry out a TIBER-EU test."[7]

Red, white, blue – how I test you

The test phases are conducted under the premise of confidentiality and ethical hacking. This means, as described above, that the RT performs its testing without the knowledge of the test subject's security or response capability (i.e., the Blue Team) and only a select circle of persons from the test subject (i.e., the White Team) will be permitted to know about the test or the TTPs to be employed. Board involvement is crucial throughout the various stages of the test.

From an organisational perspective, various specifications must be made to ensure that confidentiality can be maintained. The compliance and governance functions play an essential role in this respect. Not only do they have a validation role in the process described above, but from an organisational perspective, they must keep track of who knows about the tests and who does not. That list will have to be kept in a secure yet sufficiently manageable fashion, reflective of global locations of personnel and stakeholders and may need to be disclosed, as part of evidencing strength of testing itself, to competent supervisors. The tests must be disclosed because authorities and their respective "TIBER Cyber Teams" (**TCT**) can invalidate tests if there is evidence that they were not conducted in accordance with the framework. The TCT maintains the TIBER-EU framework and any implementation guides as well as supporting the testing entity during the test process.

Test results however, even if formally submitted to the ECB in its central bank capacity, may relevant in supervisory dialogue with ECB-SSM supervised firms.

The TIBER-EU framework is built on a “mandatory three phase process”[8]. This is comprised of:

1. Preparation phases and formal test launch - including engagement, scoping and procurement activity of Tis and RT providers as well as the setting up and approval of test parameters by the test subject's board (or presumably a similar governance function) as well as subsequent validation by the oversight/supervisory authority. Typically this could take four to eight weeks.

2. Testing phase: which includes Tl and RT probing, the delivery of a formal "Targeted Threat Intelligence Report" (the **TTI Report**) detailing the test subject's vulnerabilities, attack scenarios etc. and which will form the basis of the RT provider carrying out intelligence-led read teaming of" ... specific critical live production systems, people and processes that underpin the entity's critical functions." In short, the TTI Report lays the roadmap to going to for the jugular and testing resilience against a range of "break the business scenarios". A realistic definition of various processes relevant to and important for the breadth of the test subject's critical functions will play an important part as part of this exercise. Typically, the TTI Report may take four weeks to complete and the red teaming could take up to twelve weeks.

3. “Closure” phase: which includes compiling a "Red Team Test Report" detailing what was tested, how along with finding and observations as well as roads for improvement and remediation. The Red Team Test Report is expected to be acted upon in "...close consultation with the supervisor and/or overseer". A separate "Blue Team Report"[9] as well as a joint team, i.e., "Purple Team Replay Workshop"[10] plus 360-degree feedback[11], which aims to assist in working through the steps for improvement in, as the framework puts it: ... "a "learning and evolving" principle that

[6] See 1.4 of TIBER EU.
[7] See 6.3 of TIBER EU.
[8] See 4.2 of TIBER EU.
[9] See 10.2 of TIBER EU
[10] See 10.3 of TIBER EU
[11] See 10.4 of TIBER EU

underlies the TIBER-EU framework." Typically, the replay and remediation planning phase and sharing of practices could take six weeks to many months.

The White Team – the test watchers

In December 2018 the ECB published its TIBER-EU White Team Guidance (the **WTG**)[12]. A White Team is the team within the firm being tested and is responsible for the overall planning and management of the test, in accordance with the TIBER-EU framework. The White Team are the only persons that know a TIBER-EU test is taking place and act as the firm's invigilator during the three phases discussed above. White Teams are also responsible for ensuring that a test maximises the Blue Team's ability to learn during and from the tests.

White Team members must closely cooperate with the TIBER Test Manager from the relevant regulatory authority and the TCT. White Teams also need to cooperate with third parties, in particular where these may be members of or otherwise providing support to the Blue Team. The ECB WTG published the following principles and criteria for White Teams' inclusion and pre-clearance by the TCT.

White Team members should involve wider specific subject matter expertise, such as procurement and legal expertise as they may be needed and be required to ensure the White Team's confidentiality and sign non-disclosure agreements (**NDA**). A key priority in the WTG is on retaining the right "White Team Lead" (plus relevant deputy) in addition to all White Team members having the right level of authority and cyber (IT, red-team and cyber-resilience testing) and other technical expertise. This includes proven technical expertise in as well as the non-technical duties expected of it in terms of people management and proven experience with project management, C-level communication, crisis management, procurement and vendor management. In practice this experience should be representative of the diverse areas of the relevant entity being tested not only so as to ensure representative testing, but also to ensure certain critical business infrastructure and deliverables are not adversely affected.

A White Team Lead may also be delegated to a party that is unrelated to the entity being tested. In such instances, in addition to needing to sign an NDA, such an "external White Team Leader" cannot work for a Threat Intelligence or Red Team provider procured for the TIBER-EU framework. Lastly the WTG suggests limiting the White Team composition to less than five functions and subject matter experts with relevant cyber-skill and operational expertise. These may include the chief operating officer (COO) or other governance and/or executive function staff such as the chief information security officer (CISO) or chief technology officer (CTO) as they will not likely be involved in the day-to-day operations of the test or be part of the Blue Team. Moreover, they are also unlikely, certainly in the views of the ECB, to be the White Team Lead as instead their presence is to act as liaison between the White Team and the entity's board as well as to be responsible for agreeing the scope and signing of attestation on behalf of the entity.

Interplay of TIBER-EU with other workstreams

TIBER-EU builds upon the mandate of the ECB (as central bank) in the context of the work being advanced by ECRB, including the work around in the rules in CROE, which TIBER-EU supplements. The ECRB operates on the basis of voluntary membership and aims, in relation to cyber-resilience, to identify strategic issues, work priorities, common positions, directions and statements, as well as responding to requests for advice from national and EU authorities, including Europol and separately the somewhat controversial European Union Agency for Network & Information Security (**ENISA**) that is responsible for wider cyber-security in addition to the EU's Cyber-Security Competence Centre (**ECCC**), which is the EU's newest body to coordinate funding in cybersecurity.

The ECB also operates a TIBER-EU Knowledge Centre (**TKC**), which will have an overview of which jurisdictions have adopted TIBER-EU and act as the central gatekeeper of the framework and interlocutor of the ECRB. The ECB-hosted TKC aims to coordinate collaboration among national and European TCTs and it remains to be seen whether this will also extend to cooperation with the ECCC and ENISA.

In-scope entities should also consider that under the EU's General Data Protection Regulation (**GDPR**) has been enforced, all persons handling personal data need to ensure that adequate security measures are in place to protect this data. Hundreds of fines, including for insufficient technical and organizational measures

[12] Available here

to ensure information security, insufficient legal basis for data processing, and non-compliance with general data processing principles. Regardless of types of cyber-attack firms are, pursuant to GDPR, must maintain a robust and resilient security approach to mitigate impacts of any potential attack. In the past, regulators have imposed fines in response to incidents that reflect the extent of cybersecurity measures the impacted person had in place. Where regulators find a firm had adequate security measures in place but were nevertheless breached fines could be reduced. Consequently, where firms have insufficient measures in place, fines could be higher. Therefore, ensuring all possible prevention measures are taken will not only reduce the risk of an incident, it could also reduce regulatory fines following an incident.

Outlook and next steps

The TIBER-EU framework is similar in structure to the Banking Union. The ECB thus assumes a leading supervisory role at the international level. At the national level, supervisors will complement it accordingly. Since 2018, certain national authorities were quick to embrace TIBER-EU and some were more hesitant.

Germany, for example, decided to implement TIBER-EU in August 2020 (**TIBER-DE**)[13]. The Bundesbank and the Federal Ministry of Finance have decided to take a voluntary, cooperative approach to the implementation of TIBER-DE. Thus, it is not a measure prescribed by financial supervisors, and it encourages entities to independently and self-critically assess the cyber resilience of their systems. Much like in other European countries, Germany's implementation of TIBER-EU comprises an organizational structure that – legal obligations notwithstanding – involves financial supervisors at certain points. It also gives entities a large degree of freedom and independence in testing and enhancing their own critical functions. Within this structure, Germany's competence centre – the TCT – is based at the Bundesbank's Directorate General Payments and Settlement Systems and is thus firmly ring-fenced from the Bundesbank's financial supervision units. The TCT supports each TIBER-DE test and confirms compliance with the requirements once it has been conducted. As such, financial supervisors' involvement during a TIBER-DE Test is generally limited. Any involvement of financial supervisors shall be done via the TCT, which serves as the point of contact for the German Federal Financial Supervisory Authority (**BaFin**, in particular its IT supervision group GIT). BaFin then acts as the contact point for all other financial supervisory bodies.

Outside of Germany, and in general, the notion of the ECB-hosted TCK as a hub that coordinates multiple colleges of TCTs is also unsurprising but may translate into increased need for firms to be clear as to what is documented where and what is disclosable to whom. Equally, whilst the jurisdiction agnostic and flexible framework permits flexible adoption of the framework, which in the current version allows for relevant authorities to mandate "voluntary" testing and/or mandatory testing, may mean that firms have more disclosure channels to manage. More importantly, the TIBER-EU framework currently, even if it does very much cater for cross-jurisdictional approaches, does not contain definitive rules that deal with disagreements where stakeholders disagree on whether a critical function is in fact critical.

In summary, TIBER-EU in its current version, is a defining contribution to improved cyber-resilience. It is good for the financial system as a whole when resilience testing spreads and is performed with a more consistent methodology. At a time when testing resilience is becoming a valued part of risk management, it will be key to avoid multiple frameworks and requirements and to work toward more consistent international approaches that can rapidly improve firms' cyber-resilience capabilities and defences.

About us

PwC Legal is assisting a number of financial services firms and market participants in forward planning for changes stemming from these proposals.

[13] Available here.

If you would like to discuss any of the developments mentioned above, or how they may affect your business more generally, please contact any of our key contacts or PwC Legal's RegCORE Team via de_regcore@pwc.com or our website.

Dr. Michael Huertas
Tel.: +49 160 973 757-60
michael.huertas@pwc.com

www.pwclegal.de