RegCORE Client Alert

Revisiting the ECB's rules for selecting service providers for cyber-resilience testing

September 2021

ECB Procurement Guidelines

Revisiting the ECB's rules for selecting service providers for cyber-resilience testing

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

Contact RegCORE Team
de_regcore@pwc.com

On 2 May 2018 the European Central Bank (**ECB**) published its framework for "Threat Intelligence-Based Ethical Red-Teaming" (**TIBER-EU**) Framework[1]. This framework describes a controlled and tailored testing approach to increase the resilience of digital networks of financial services firms and the entire financial sector across the EU. Here, the ECB did not just act as a supervisory authority of the Banking Union but in its function as a central bank. Under the new rules, TIBER-EU tests are run using intelligence-based ethical hacking. Covered by the scope under this "voluntary" regime are public authorities, but also financial services companies and financial market infrastructure providers. Covered entities are expected to incorporate a "comply or explain" approach to the TIBER-EU Framework and when engaging service providers to conduct the relevant tests.

In principle, only cyber resilience testing performed by Red Team Testing (**RT**) and Threat Intelligence (**TI**) service providers will be recognised by the TIBER-EU Framework. These must be selected and contracted in accordance with the "TIBER-EU Framework Services Procurement Guidelines" (the **Procurement Guidelines**)[2]. This Client Alert discusses the current version of the Procurement Guidelines' requirements and the ECB's expectations and should be read in conjunction with our Client Alert on the TIBER-EU framework from 15 September 2021. The Procurement Guidelines complement existing EU and national rules on selecting and commissioning of service providers and will also likely be of relevance ahead of the introduction of the new EU's proposal for a new regulation for a digital operational resilience act (**DORA**) which is expected to take operational effect from 2024[3].

In particular, regulated entities that have a strong compliance program for regulated outsourcing and delegation arrangements will be familiar with the contents of the TIBER-EU Framework. The ECB, however,

[1] Available here
[2] Available here
[3] 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).

has different requirements and expectations that can be quite technical and prescriptive. As with similar ECB regulatory instruments or other guidance that can read like rulebooks, the TIBER-EU Framework and Procurement Guidelines use the verb "should", which should be read to mean "shall" or "must". It is also of interest to note that neither the TIBER-EU Framework nor the Procurement Guidelines refer to, for example, the "Cyber Lexicon" of approximately 50 core cybersecurity and cyber resilience terms, launched by the Financial Stability Board on 2 July 2018. This may be useful for certain firms needing to meet cyber-resilience rules across multiple jurisdictions.

What do the Procurement Guidelines require?

The Procurement Guidelines specifically emphasise that entities covered by the scope, and in particular those planning to apply the TIBER-EU framework to their global activities, must comply with all obligations that apply to them. The Procurement Guidelines are currently split into the following three parts:

1. Establish requirements and standards that RT/TI providers must meet to deliver recognised TIBER-EU tests;

2. Offer guiding principles and selection criteria that in-scope entities should observe, in addition to requirements in respective and applicable legal and regulatory requirements, when procuring services from prospective RT/TI providers; and

3. Provide questions and checklists relevant for contractual arrangements that entities are free to apply in their due diligence and when formalizing the procurement process with RT/TI providers.

The role of the TI provider

To meet the requirements of the TIBER-EU framework, institutions must collect accurate threat intelligence when conducting effective cyber resilience red-teaming and risk assessment. TI providers are essential here. The Procurement Guidelines explicably state:

> “Creating accurate and realistic threat intelligence is a complex activity. This means that the TI provider must have adequate knowledge of the threat actors, their motives and their TTPs [tactics, techniques and procedures], as well [as] an understanding of how the core elements of the financial system interact and operate. In addition, the TI provider must have a good insight into the targeted entity. It needs to know for example: what the target’s critical functions are; how the target operates; who the crucial employees are and whether they are “usable” for the attack; and what the target’s vulnerabilities are.”[4]

Comprehensive threat intelligence is therefore of enormous importance because it provides the TI provider with high-quality information. This information enables him to simulate a realistic attack on those live systems of the institution that support the "critical functions" and their cyber resilience. These tests are consistent with the ethos of the TIBER-EU framework. Whether and when tests based on TIBER-EU are carried out is a matter for the respective authorities and stakeholders themselves to decide. According to the procurement guidelines, the TI provider must meet the following qualitative requirements. It is also noted that, to the extent possible, only accredited and certified providers should be selected.

According to the Procurement Guidelines, the ECB expects in-scope entities to:

I. Document the due diligence conducted prior to selecting a provider –preferably using the questions in the Annex

II. Evidence how TI providers meet the following requirements in the table below

III. Monitor and record how the TI provider performs against key performance indicators in service level agreements.

The following outlines requirements for the individual functions within the different firms.

Function: The TI provider (at company level)

[4] See 3.2 of the Procurement Guidelines (August 2013)

Requirements to be fulfilled by TI provider according to Procurement Guidelines:

- At least three references from previous assignments related to threat intelligence-led red team tests
- Adequate indemnity insurance in place to cover activities that were not agreed up on in the engagement and service level arrangements and/or which stem from misconduct, negligence etc.
- Evidence a robust understanding and application of information governance, security and risk management
- Adhere to professional codes of conduct such as the Code of Conduct for Ethical Security Testers or the Open Source Intelligence and Research Association's -OSIRA Code of Conduct

Function: The TI provider's Threat Intelligence Manager (the TIM) designated for the TIBER-EU test and responsible for its end-to-end management

Requirements to be fulfilled by TIM according to Procurement Guidelines:

- The TIM leads and has oversight of the TI provider's activities for delivering a TIBER-EU test
- The TIM must have sufficient experience in threat intelligence – the expectation is at least five years of experience in threat intelligence, of which at least three years are in producing threat intelligence in the financial services industry
- The TI provider will provide:
  - a current CV of the TIM and at least three references in relation to the TIM's work on previous assignments and specifically red team testing
  - background checks on the TIM – which may be simplified and/or enhanced disclosure
- The TIM must have appropriate recognised qualifications and certifications (as set out in Annex 1 to the Procurement Guidelines)

Function: The TI provider's Threat Intelligence Team (the TI Team) (all members other than TIM responsible for delivering the TIBER-EU test)

Requirements to be fulfilled by TI Team according to Procurement Guidelines:

- The TI Team must collectively evidence sufficient experience and each member must have at least two years of experience delivering threat intelligence services
- The TI provider must provide a current CV for each team member as well as background checks
- The relevant team composition should be multi-disciplinary and evidence a broad range of skills, including "OSINT, HUMINT and geopolitical knowledge." OSINT refers to open source intelligence gathering of information derived from public and/or predictive sources. HUMINT refers to "human intelligence" gathering of data. The Procurement Guidelines' "Recommended Questions" also refer to SIGINT i.e., signals intelligence capabilities
- Ideally the team members are expected to have appropriate recognised qualifications and certifications for threat intelligence and professional experience in delivering threat intelligence for red team tests

The Procurement Guidelines comprehensively describe the characteristics that the TI provider must adhere to when generating threat data. In turn, the report to be created on the threat data must be delivered in a way that complies with the EU General Data Protection Regulation (**GDPR**).

The role of the RT provider

The RT provider's task is to plan and conduct the TIBER-EU testing of the institute's systems, processes, technologies, and personnel through which the exercise is targeted. The basis of the test is the TI provider's report. The difference from usual resilience tests is that it imitates the tactics of the real attacker who wants to attack the critical functions of the institution. The Procurement Guidelines thus clearly establish the expectation that RT and TI providers will collaborate in the creation of the Red Team test plan and before, during, and after the actual test phase and then in the creation of the report.

According to the Procurement Guidelines, the RT provider must meet the following requirements:

- At least five references from previous assignments related to intelligence-led red team tests
- Adequate indemnity insurance in place to cover activities that were not agreed up on in the engagement and service level arrangements and/or which stem from misconduct, negligence etc.

- Evidence a robust understanding and application of information governance, security and risk management
- Adhere to professional codes of conduct such as the Code of Conduct for Ethical Security Testers or the Open Source Intelligence and Research Association's -OSIRA Code of Conduct

Function: The RT provider's Red Team Test Manager (the RTTM) designated for the TIBER-EU test and responsible for its end-to-end management

Requirements to be fulfilled by RTTM according to Procurement Guidelines:

- The RTTM leads and has oversight of the TI provider's activities for delivering a TIBER-EU test
- The RTTM must have sufficient experience in red team testing – the expectation is at least five years of experience in testing, of which at least three years are in leading red team tests in the financial services industry
- The RT provider will provide:
  - A current CV of the RTTM and at least three references in relation to the RTTM's work on previous assignments and specifically red team testing
  - Background checks on the RTTM – which may be simplified and/or enhanced disclosure
- The RTTM must have appropriate recognized qualifications and certifications (as set out in Annex 1 to the Procurement Guidelines)

Function: The TI provider's Red Team (all members other than RTTM responsible for delivering the TIBER-EU test

Requirements to be fulfilled by TI provider's Red Team according to Procurement Guidelines:

- The Red Team must collectively evidence sufficient experience, and each member must have at least two years of experience delivering red team testing
- The RT provider must provide a current CV for each team member as well as background checks
- The relevant team composition should be multi-disciplinary and evidence a broad combination of skills, including reconnaissance, threat intelligence, risk management, exploit development, vulnerability analysis, penetration testing, social engineering etc.
- Ideally the team members are expected to have appropriate recognized qualifications and certifications

The focus of the procurement guidelines is on TI providers, but also on the multilingualism of RT providers and that the fact that they have extensive experience, particularly in the financial services sector. This aims to ensure that providers can borrow tactics and adapt these to TIBER-EU tests.

One of the reasons for focusing on multilingualism is that the language used in simulated attacks must also be used in a plausible manner so that the simulated fraudulent attacks to obtain sensitive data are authentic and as close to reality as possible. Recommended questions and checklists

The Annex to the Procurement Guidelines contains a list of certifications and qualifications that relevant team members at RT/TI providers should demonstrate and recommended questions that in-scope entities can use when selecting providers. Specific requests, which may go beyond existing EU and national level requirements, are for the provider to supply its recruitment policy and process or for providers to also disclose details/results of independent audits of its information security system.

The Annex also lists requirements and content that must be included in the service agreement that must be entered into with the respective RT/TI provider. The focus is on detailed information security measures and screening of employees to be put in place, detailed measures on whom information can be shared with and when as well as incident response management, continuity of services and exit clauses as they relate to data destruction and more generally.

Outlook and Latest developments

The Procurement Guidelines represent only one part of the TIBER-EU framework. Although the Procurement Guidelines are quite prescriptive in parts, they have the advantage of setting targets and enabling customers and service providers to work together on standardised terms. For in-scope entities much of the compliance challenge will likely be in ensuring that the selection and decision-making process when retaining providers meets the expectations set in the TIBER-EU Framework. Depending on the extent of measures in place, it may be prudent to diligence relevant existing providers anew so as to meet the expectations of the Procurement Guidelines formally. For RT/TI service providers the Procurement Guidelines present an opportunity to have a much more structured roadmap on compliance expectations and service level performance monitoring.

Lastly, the ECB may over time become more vocal on where RT/TI providers corporate domicile are located or where the testing facilities are located. This could mean that more specific expectations are communicated beyond "just" the requirement to comply with GDPR or evidence sufficient multilingual capabilities—read proficiency in one or more languages of the EU.

As part of the EU's Digital Finance Strategy[5], DORA is designed to consolidate and upgrade ICT risk requirements across financial institutions to ensure a common standard regarding ICT risks. DORA thus also builds on the TIBER-EU framework although there are a number of parts that will need to be adapted in the legislative frameworks but also for firms in how they deal with their RT/TI providers. Importantly, the draft version of DORA provides for six areas of action that cover almost the entire spectrum of ICT risk management and entail corresponding adaptation efforts on the part of financial service providers: ICT risk management, reporting, resilience testing, third-party ICT risks, information exchange and governance. As things stand, the topics with most changes are likely to be third-party ICT risks and resilience testing. For example, outsourcing in the future will require consideration of third-party concentration risk, identification and special oversight of partners involved in critical functions, and modified contract design. Regulators' rights of enforcement over third-party vendors are growing significantly, up to and including the right to order termination of contracts. Penetration and stress tests can be expected to increase in frequency, but there will also be a greater focus on quality.

DORA is expected to come into force during the first half of 2024, with secondary legislation immediately following. Financial services firms are advised to start familiarising themselves with the new rules and to watch this space for any new updates coming as well as to possibly ensure that they engage early with their RT/TI providers.

About us

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

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

[5] Available here

© 2022 PricewaterhouseCoopers Legal Aktiengesellschaft Rechtsanwaltsgesellschaft. All rights reserved.

In this document, “PwC Legal” refers to PricewaterhouseCoopers Legal Aktiengesellschaft Rechtsanwaltsgesellschaft, which is part of the network of PricewaterhouseCoopers International Limited (PwCIL). Each member firm of PwCIL is a separate and independent legal entity.

www.pwclegal.de