EUROPEAN CENTRAL BANK

EUROSYSTEM

TIBER-EU Framework

Services Procurement Guidelines

August 2018

Contents

1 Executive summary

The Threat Intelligence-based Ethical Red Teaming (TIBER-EU) Framework enables European and national authorities to work with financial infrastructures and institutions (hereafter referred to collectively as "entities"[1]) to put in place a programme to test and improve their resilience against sophisticated cyber attacks.

The ECB published the TIBER-EU Framework *(TIBER-EU Framework: How to Implement the European Framework for Threat Intelligence-based Ethical Red Teaming)*[2] *in* May 2018. The present Services Procurement Guidelines ("Guidelines") are referred to in, and are an integral part of, the TIBER-EU Framework. They set out in detail the different elements of TIBER-EU procurement. TIBER-EU is an instrument for red team (RT) testing, designed for use by core financial infrastructures, whether at national or at European level, which can also be used by any type or size of entity across the financial and other sectors[3]. At the same time, TIBER-EU is designed to be adopted by the 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. When an authority adopts TIBER-EU, tests will only be considered TIBER-EU tests when they are conducted in accordance with TIBER-EU including these Guidelines.

TIBER-EU facilitates RT testing for entities which are active in more than one jurisdiction and fall within the regulatory remit of several authorities. TIBER-EU provides the elements allowing either collaborative cross-authority testing or mutual recognition by relevant authorities on the basis of different sets of requirements being met[4].

Due to the inherent risks associated with RT testing, also present in TIBER-EU tests, TIBER-EU includes as a key element for risk management the use of the most competent, qualified and skilled threat intelligence (TI) and RT providers with the necessary experience to conduct RT tests. Consequently, prior to engagement with potential TI and RT providers with a view to performing a TIBER-EU test, the relevant entity has to take into account the requirements of the Guidelines and in particular those regarding such providers. These requirements are deliberately stringent to mitigate risks including those related to RT tests being conducted by inexperienced personnel, which could have an adverse impact on the relevant entity.

---

1 For the purposes of the TIBER-EU Framework, "entities" means: payment systems, central securities depositories, central counterparty clearing houses, trade repositories, credit rating agencies, stock exchanges, securities settlement platforms, banks, payment institutions, insurance companies, asset management companies and any other service providers deemed critical for the functioning of the financial sector.

2 TIBER-EU FRAMEWORK, How to implement the European framework for Threat Intelligence-based Ethical Red Teaming.

3 TIBER-EU, point 1.4.

4 TIBER-EU, point 1.4.

1.1 What is TIBER-EU?

TIBER-EU is a framework that delivers a controlled, bespoke, intelligence-led red team test of entities' critical live production systems. Intelligence-led red team tests mimic the tactics, techniques and procedures (TTPs) of real-life threat actors who, on the basis of threat intelligence, are perceived as posing a genuine threat to these entities. An intelligence-led red team test involves the use of a variety of techniques to simulate an attack on an entity's critical functions (CFs) and underlying systems (i.e. its people, processes and technologies). It helps an entity to assess its protection, detection and response capabilities.

1.2 What are the risks of the TIBER-EU test?

There are inherent elements of risk associated with a TIBER-EU test for all parties due to the criticality of the live production systems, people and processes involved in the tests. The possibility of causing a denial-of-service incident, an unexpected system crash, damage to critical live production systems, or the loss, modification or disclosure of data, highlights the need for active and robust risk management. In line with the potential risk of the test, the TIBER-EU Framework gives a high priority to establishing robust risk management controls throughout the entire process of the test to ensure it is conducted in a controlled manner.

To ensure a controlled and safe test, one prescribed control is the use of specialist external threat intelligence (TI) and red team (RT) providers, which have the highest level of skills and expertise, and have the requisite experience in threat intelligence and red team testing in the financial services industry to be able to deliver effective and cutting-edge professional services. External providers provide a fresh and independent perspective and are likely to have more resources and up-to-date skills to deploy, which would add value to the entity.

1.3 What are the Services Procurement Guidelines?

The Guidelines set out in detail the different elements of TIBER-EU procurement. They are an integral part of the TIBER-EU Framework. The Guidelines are divided into three parts. They:

- set out the requirements and standards that must be met by TI and RT providers to deliver recognised TIBER-EU tests;
- offer guiding principles and selection criteria for entities, as they look to procure services from prospective providers; and
- provide questions and agreement checklists that could be used when entities undertake their due diligence and look to formalise the procurement process with the TI/RT providers.

As entities go through the procurement process, they are encouraged to seek further clarification of the selection criteria, TI and RT provider requirements and any other aspects related to the conduct of a TIBER-EU test. During the procurement process, entities are also encouraged to engage in constructive dialogue with potential TI/RT providers, allowing the entities to gain a deeper understanding of the TI/RT providers' capabilities.

Further details of the TIBER-EU Framework can be found in the document TIBER-EU Framework: How to implement the TIBER-EU Framework[5]. Any further enquiries about TIBER-EU should be sent to TIBER-EU@ecb.europa.eu.

[5] TIBER-EU FRAMEWORK, How to implement the European framework for Threat Intelligence-based Ethical Red Teaming.

2 Introduction

2.1 Use of the Services Procurement Guidelines

Due to the sensitive nature of TIBER-EU tests, entities need to carefully select TI and RT providers which can provide an appropriate level of professional expertise and support for conducting the test.

The market for threat intelligence and red team testing varies widely, with many providers providing an array of services. It is important that entities take due care during their procurement process. It is therefore recommended that entities and the TIBER Cyber Teams (TCTs) work in close collaboration with TI/RT providers, to ensure that a standardised and consistent approach is followed in using the services of TI/RT providers, and that there is a common understanding of the standards required to perform such tests. Following the Guidelines will allow their target audience (Section 2.3) to make sure that the requirements for TI/RT providers to deliver TIBER-EU tests are met.

As the TIBER-EU Framework is operationalised across the European Union (EU), the TIBER-EU Knowledge Centre (TKC) will monitor the evolution of the threat intelligence and red team testing market and update the requirements, if necessary. The TKC will undertake this task by closely liaising with the authorities that adopt the TIBER-EU Framework, the entities that undertake the tests and the TI/RT providers that deliver the tests.

2.2 Structure of the Guidelines

The Guidelines are structured as follows:

- Section 3 sets out the requirements and standards that must be met by TI providers to deliver recognised TIBER-EU tests, and offers guiding principles and selection criteria for entities, as they look to procure services from prospective providers.
- Section 4 sets out the requirements and standards that must be met by RT providers to deliver recognised TIBER-EU tests, and offers guiding principles and selection criteria for entities, as they look to procure services from prospective providers.
- Section 5 provides guidance to authorities that are looking to implement TIBER-EU at national and European level, with specific regard to procurement.
- Annex 1 provides a list of certifications that staff members and providers may be, depending on the case, required to possess. Annexes 2-5 provide specific questions that entities could use when considering prospective providers and

agreement checklists to assist the procurement functions during their procurement process, respectively.

2.3 Target audience of the Guidelines

The Guidelines are directed at:

- authorities responsible for the adoption, implementation and management of the TIBER-EU Framework at national and European levels;
- entities looking to undertake TIBER-EU tests;
- organisations interested in providing cyber threat intelligence services under TIBER-EU;
- organisations interested in providing red team testing services under TIBER-EU; and
- accreditation and certification providers.

2.4 Multinational entities

Although the Guidelines set out the requirements for TI and RT providers in the EU conducting TIBER-EU tests, there are multinational entities that may need to conduct such tests beyond the EU or in collaboration with other non-EU relevant authorities that implement their own red team testing framework.

In such circumstances, the entities in question should understand the requirements of the authorities in the other relevant jurisdictions and, furthermore, they are encouraged to analyse the authorities' respective requirements. This is particularly important if the entity wishes to use the results of the test to satisfy the requirements of authorities from other jurisdictions. In such cases, the entity should liaise with all relevant authorities, which may provide guidance to the entity on the procurement requirements. For example, some jurisdictions may mandate the validation of expertise by accreditation and certification providers. Entities should seek to confirm their approach meets all involved jurisdictions' requirements at the scoping stage of the process. In all cases, the requirements set out in this document are the minimum standards that must be met to achieve a recognised TIBER-EU test.

2.5 Procurement agreements

In some cases, entities may be party to an agreement with a provider or range of providers that enables them to place orders for different types of services without running lengthy, full tendering exercises. In such cases, if the entity opts to use its agreement to procure TI and RT providers to conduct TIBER-EU tests, the prospective TI/RT providers must meet the requirements set out in these Guidelines.

In cases where such agreements are in place, the entity should liaise with the relevant TCT for further clarifications.

3 Threat intelligence providers

Threat intelligence-based scenarios mimicking real-life cyber adversaries are essential to the success of TIBER-EU testing activities. Threat intelligence provides a detailed view of the specific entity's attack surface and helps produce actionable and realistic testing scenarios. Such test scenarios look to emulate the tactics, techniques and procedures (TTPs) of real-life threat actors within a threat landscape and will be used to deliver a realistic simulation. Threat intelligence will be used by the RT provider to develop attack scenarios and execute an intelligence-led red team test of specified critical live production systems, people and processes that underpin the entity's critical functions (CFs). These scenarios will be integrated into the RT provider's Red Team Test Plan and help the RT provider to deliver a practical assessment of the entity's protection, detection and response capabilities.

This section provides an overview of the role of threat intelligence and TI providers in the TIBER-EU context; sets out the core requirements of a TI provider delivering services for a recognised TIBER-EU test; and describes the guiding principles and criteria for the entity to consider when procuring a TI provider.

3.1 Threat intelligence for TIBER-EU

TIBER-EU defines a threat as:

- an expression of intent to do harm, deprive, weaken, damage or destroy;
- an indication of imminent harm;
- an agent that is regarded as harmful; and
- a harmful agent's actions comprising TTPs.

TIBER-EU defines threat intelligence as "information that provides relevant and sufficient understanding for mitigating the impact of a potentially harmful event". Threat intelligence encompasses: (1) the technical details of the attack (indicators of compromise, or the what, when and where); (2) the TTPs behind the attack (the modus operandi or how); and (3) the details of the attackers themselves and their motivations (the who and why).

Within this context, threat intelligence-based scenarios mimicking real-life cyber adversaries are essential to the success of testing activities. There are two complementary tools to develop these threat intelligence-based scenarios: the Generic Threat Landscape (GTL)[6] Report and the Targeted Threat Intelligence (TTI)

[6] The GTL Report is not necessarily to be procured by the tested entity; it could be a joint procurement by a subset of national financial sectors or by the European financial sector. Alternatively, the lead authority could take responsibility for delivering the GTL Report.

Report. The GTL Report should reflect the most significant threats faced by the financial sector, whether at a national or European level. The GTL Report can be used to develop the TTI Report, which gives a more detailed view of the specific entity's current defences and attack surface and helps produce actionable and realistic attack scenarios. Such attack scenarios look to emulate the TTPs of real-life threat actors within a threat landscape and will be used to deliver a realistic simulation.

3.2 The role of the TI provider

The TI provider has a crucial role in the TIBER-EU process. It should provide the RT provider with a TTI Report that formulates threat scenarios aimed at mimicking potential threat actors' attacks against the live systems that underpin the critical functions of an entity. These threat scenarios form the basis of the attack scenarios the RT provider will deliver.

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 skills and TTPs, as well 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.

All this will provide the RT provider with the information needed to simulate a real-life and realistic attack on the entity's live systems underpinning its critical functions.

Collecting and analysing all this information and converting it into threat intelligence require specialised skills and expertise. The TI provider must also have robust risk management and security controls in place, as such threat information about an entity is highly sensitive and may pose a threat to the entity, if the information falls into the wrong hands.

3.3 TI provider requirements

To ensure that the TI provider is able to furnish the deliverables cited above in an effective and safe manner, it must display the highest standards. Consequently, the TIBER-EU Framework requires TI providers to meet specific requirements to also ensure that the test is recognised by the relevant authorities. The core requirements below are set to ensure that only the highest-quality providers, with sufficient experience and capabilities, can contribute to red team tests on the most critical functions of entities. These requirements are without prejudice to the application of all relevant EU and national data protection regulations and other rules.

All TIBER-EU tests will require a Threat Intelligence Team, composed of a Threat Intelligence Manager and other Threat Intelligence Team members, with a broad set of skills and experience. The size of the Threat Intelligence Team will depend on the entity being tested, the scope of the test, and the specific skills and expertise required to deliver the test.

Table 1

TI Provider requirements to deliver TIBER-EU tests

Who	Requirements
TI provider (at company level)	At least three references from previous assignments related to threat intelligence-led red team tests Adequate indemnity insurance in place to cover activities which were not agreed upon in the contract and/or which stem from misconduct, negligence, etc.
Threat Intelligence Manager – responsible for the end-to-end management of the threat intelligence for a TIBER-EU test	Lead and oversight of the TI provider's activities for delivering a TIBER-EU test are ensured by a Threat Intelligence Manager Sufficient experience of the Threat Intelligence Manager in threat intelligence. Expectation: at least five years of experience in threat intelligence, including three years of producing threat intelligence in the financial services industry Up-to-date CV and at least three references from previous assignments of the Threat Intelligence Manager to be provided to the entity, specifically in delivering threat intelligence for red team testing activities Background checks on the Threat Intelligence Manager are conducted by the TI provider (as a minimum). Enhanced background checks are conducted as required by the national authorities Ideally, the Threat Intelligence Manager should have appropriate recognised qualifications and certifications for threat intelligence (as set out in Annex 1)
Threat Intelligence Team (all members of the team, except for the Threat Intelligence Manager) – responsible for delivering the threat intelligence for a TIBER-EU test	Sufficient experience of the Threat Intelligence Team members. Expectation for each member: at least two years of experience in threat intelligence Up-to-date CV for each member of the team to be provided to the entity Multi-disciplinary composition of the Threat Intelligence Team, with a broad range of skills including OSINT, HUMINT and geopolitical knowledge Background checks on each member of the Threat Intelligence Team are conducted by the TI provider (as a minimum). Enhanced background checks are conducted as required by the national authorities Ideally, the Threat Intelligence Team members should have appropriate recognised qualifications and certifications for threat intelligence (as set out in Annex 1) Ideally, the Threat Intelligence Team should have experience in delivering threat intelligence for red team tests

It is the responsibility of the entity to ensure that the TI providers meet these requirements prior to formalising any test, and therefore it should undertake thorough due diligence during its procurement process.

However, it is recommended that the entity delegate this responsibility to accreditation and certification bodies in the EU. As soon as there is sufficient capability in the EU to conduct TIBER-EU accreditation and certification of TI providers and their staff, respectively, the entity should opt for only TIBER-EU accredited and certified TI providers[7]. The Services Procurement Guidelines will be updated by the TIBER-EU Knowledge Centre when such capability is deemed to be in place.

[7] The accreditation and certification provider validates the baseline level of proficiency of the TI provider and its staff to provide threat intelligence services.

3.4 Guiding principles and criteria for selecting TI providers

This section sets out the guiding principles and criteria for the entity to consider during its procurement process and when evaluating the capabilities of a TI provider. These principles are of a more qualitative nature than the requirements set out in Section 3.3, and thus entities should look to integrate these principles and criteria in their request for proposals and bilateral discussions with prospective providers, aided by the questions in Annex 2.

TI provider's reputation, history and ethics

Three of the most important criteria for a buyer of threat intelligence services are the reputation and history of the TI provider and the ethical conduct it both adopts and enforces.

A suitable and reputable TI provider should be able to clearly demonstrate its knowledge and expertise in threat intelligence and in the financial services industry more generally. This should be focused on highlighting areas where risk to the entity can be minimised – such as understanding the legal and ethical challenges.

Mature and capable TI providers are generally those that have conducted multiple assignments already for a broad range of entities in different jurisdictions; have first-hand experience of the issues and complexities involved; have a good depth and breadth of experience and knowledge of the financial services industry; and have appropriate processes and capabilities to gather, analyse and produce threat intelligence on a variety of entities.

Successful TIBER-EU tests are underpinned by a collaborative, transparent and flexible working approach observed by all TIBER-EU stakeholders. TI providers must demonstrate an ability and willingness to work in this way. This entails requirements regarding the roles present in the TI provider's organisational set-up. The TI provider, as a minimum, should have:

- Threat Intelligence Managers and TI experts;
- thematic and functional analysts; and
- technical experts and support staff.

The entity should engage with potential TI providers and understand their history, organisational set-up, range of expertise and body of previous work, particularly within the financial services industry.

TI providers should be committed to ensuring that they act in a professional and ethical manner. For example, the TI provider:

- should adhere to a professional Code of Conduct, e.g. the Code of Conduct for Ethical Security Testers or the OSIRA Code of Conduct[8]; and
- should have a mature understanding of ethical standards in gathering and processing human and technical intelligence.

Information must be gathered using approaches that respect the relevant legislative framework. In particular, the law of the relevant EU Member State in which the TIBER-EU test is executed must be adhered to.

Governance, security and risk management

It is important that the TI provider gives a high priority to governance, security and risk management. A competent TI provider should be able to provide assurances that the security of and risks associated with the entity's critical systems and confidential information (together with any other business risks) will be adequately addressed. The TI provider should be able to ensure that the results of its tests are generated, reported, stored, communicated, redacted (if necessary) and destroyed in a manner that does not put entities at risk.

During any TIBER-EU test, it is likely that the TI provider will encounter sensitive or business-critical data related to the entity or its third party suppliers. The entity should ensure that the TI provider fully understands the sensitivity of this, and puts in place all the appropriate security objectives, policies and procedures to address these possible situations, including for data of the entities' third party suppliers which are in the scope of a TIBER-EU test. Overall, the entity will need to be comfortable that it can trust the TI provider.

Suitable and mature TI providers should have a robust Information Security Management System (ISMS) with a bespoke security control framework and appropriate certification, based on recognised international standards. Examples of such certifications are included in Annex 1. The ISMS should define a clear governance structure and processes, which are effectively established, implemented, operated, continuously monitored, tested, reviewed, maintained and improved.

The entity should request the TI provider to furnish evidence of its relevant internal information security policies that ensure the security and resilience of its services and methods. The entity should analyse these pieces of evidence, ensuring that they are aligned with the TI provider's high-level security objectives.

[8] Open Source Intelligence and Research Association.

Methodology

TI providers should have robust methodologies in place to develop their threat intelligence and reconnaissance. The TI provider should be able to clearly explain its methodologies, how they evolve and how they result in effective and high-quality outputs for red team tests.

The methodologies should demonstrate how the TI provider:

- is able to obtain a useful context for conducting the threat analysis;
- sources information about the current state of the entity;
- gathers evidence;
- engages with entities and other key stakeholders;
- has a comprehensive view of the financial sector and the current geopolitical context that entities operate in;
- conducts risk assessments and analysis; and
- can operationalise its methodologies in a clear, transparent and flexible manner.

The TI provider must be able to demonstrate a comprehensive threat intelligence collection process and function, which provides the raw materials for conducting threat intelligence analysis. In collecting threat intelligence, the TI provider must be able to demonstrate its ability to harvest information from a variety of source types, as these will directly influence the quality of the output.

Most collection processes and functions acquire data from a wide variety of data sources. The extent of this variety is a useful indicator of the range of intelligence that a procuring entity should expect from a TI provider. These sources include internet services, a mixture of public and private forums, and a range of media types such as IRC chats, email and video. The key characteristics of such threat intelligence collection are set out below:

Table 2

Characteristics of TI collection

Characteristics of TI collection process and function	Explanation
Breadth of sources	The number of information items in any given source type is a useful means of measuring the likely catchment capability of any collection function. A TI provider that collects across 100,000 unique information items will be expected to generate fewer results overall compared with one that collects across 30 million. That said, the classic "garbage in, garbage out" rule applies and this must, of course, be balanced against the ability of the TI provider to select information items that are likely to contain content of interest and the likely rate of false positives emanating from that source.
Depth of sources	TI providers collecting intelligence may only touch the surface content of a given source, but it is also important to know that all the content of a given source can be incorporated when there is an appropriate, and lawful, opportunity to do so. It is therefore important to assess whether a TI provider can provide the option of acquiring data at scale. By acquiring data at scale in this manner, it is possible to query the data after retrieval from its original source. This can be useful when the hypothesis, or question, is sensitive in nature.
Language support	Languages play an important role in selecting an effective TI provider. For local TIBER-EU implementations, the TI provider must have staff with proficiency in the language needed for the test (e.g. Dutch in the case of TIBER-NL, German in the case of TIBER-DE). In the case of entities that operate across multiple jurisdictions, TI providers may need to demonstrate proficiency in multiple languages, or at least be able to obtain information in any language on threat actors and convert this into actionable intelligence in the local language. Cyber threats are a global phenomenon and a TI provider that offers no coverage of major global languages will miss a significant proportion of relevant information. Therefore, TI providers with staff who can demonstrate fluency in key languages will offer a considerable advantage. This includes ensuring that the TI provider's technology and people can ingest, process and manage content in multiple languages.
Timeliness of collection	The timeliness of collection will vary from source to source. A TI provider must demonstrate its ability to absorb information from high-volume and dynamic data sources (such as Twitter) at a rate at which the intelligence is relevant at the moment it is processed and analysed. It is also useful to understand the TI provider's retention period for such information, to gauge how long the TI provider can store and interrogate this information. For example, having the ability to spot malicious tweets over a previous two-year period is more valuable than over a six-month period.
Types of intelligence	The threat intelligence market contains TI providers which employ a variety of intelligence-gathering disciplines. TI providers that use both OSINT (open source intelligence derived overtly from publicly available sources) and HUMINT (intelligence derived overtly or covertly from human sources/social engineering) are better able to gather intelligence relating to covert groups such as organised criminals compared with those that use OSINT only. TI providers that use SIGINT (signals intelligence derived, for example, from signals generated routinely by hardware devices or software applications) are more likely to gather intelligence suitable for system monitoring purposes.
Intelligence-gathering process	The TI provider's intelligence-gathering process life cycle must include review, operations management and quality management. The TI provider must provide transparency in the way intelligence is collected and ensure that it does not participate in or enable criminal activities.
Threat intelligence analysis	It is important to ensure that a TI provider employs a range of techniques to ensure the consistency, accuracy and relevance of the information resulting from this phase of the process. For example, the TI provider should be able to: • demonstrate that it has systems and processes to remove confirmation bias and other cognitive errors where results are curated by an analyst; • cross-check facts by de-duplicating and collating content into a consistent format; • employ data-driven and hypothesis-driven assessment strategies, i.e. the TI provider is capable of uncovering new intelligence by identifying patterns in the collected data and by validating hypotheses; • proactively anticipate client needs; • work productively together with the RT provider in order to develop the best possible scenarios, based on robust TI analysis; • deliver near-real-time alerts and warnings when analysis shows emerging and/or immediate threats; and • deliver specific analysis upon client request in a timely manner.
Dissemination	The final threat intelligence product disseminated to the entity should: • provide state of the art intelligence: this is information that provides relevant and sufficient understanding for mitigating the impact of a potentially harmful event, plus relevant guidance, so that an RT provider can use it to construct realistic attack scenarios; • be in an appropriate format: intelligence should be concise, clear and consistent, written in the language preferred by the procuring entity and – in the case of cross-jurisdictional entities – in English too. Outputs should avoid the use of jargon wherever possible; • offer a mechanism for prioritising and comparing results: intelligence should be graded according to the severity of the threat and the veracity and urgency of intelligence that has been found; • provide both granularity and situational awareness; and • be in line with the General Data Protection Regulation (GDPR).

Staff competence

The level of threat intelligence provided depends heavily on the staff of the TI provider. Therefore:

- staff employed by the TI provider should be of irreproachable behaviour, as demonstrated by screening of criminal antecedents;
- staff employed by the TI provider should be from a range of backgrounds and possess sufficient experience, e.g. backgrounds in governmental intelligence, law enforcement and financial services;
- the TI provider should be able to show that its recruitment process involves selection based on: analytical capabilities, technical skills, social skills, creativity and relevant financial sector experience; and
- the TI provider should promote and have mechanisms to ensure continuous professional development and an R&D culture.

Collaborative working

Successful TIBER-EU tests are underpinned by a collaborative, transparent and flexible working approach observed by both TI and RT providers. A TI provider must demonstrate a willingness to work in this way, sharing its deliverables with its RT testing counterpart for review and comment. The TI provider should also demonstrate a willingness to work with the RT provider throughout the test to ensure that the threat scenarios are transformed into a cohesive and tractable Red Team Test Plan.

Language support

Given the multinational nature of entities and the possible implementation of TIBER-EU across different jurisdictions in the EU, the TI provider should have the capability to deliver threat intelligence, perform reconnaissance and produce reports in different languages. The entity should discuss the TI provider's capabilities and resources in this regard.

In national implementations of the TIBER-EU Framework, the entity may ask the TI provider for a test report written in the local language. However, in the case of cross-border entities where mutual recognition is being sought amongst various authorities, the TI provider should be able to deliver the report written in English.

Confidentiality

The TI provider should not use information acquired in the context of TIBER-EU for services provided to other parties. Therefore, TIBER-EU information can only be

used for the purpose for which it was provided. Furthermore, due to the confidential nature of TIBER-EU tests, information must be protected against unintentional disclosure. The TI provider needs to be able to provide assurances that the security and risks associated with the confidential nature of TIBER-EU tests are being adequately addressed, in accordance with jurisdictional regulations.

The TI provider should agree with the procuring entity the protocols to destroy all sensitive information related to the entity and the outputs from the TIBER-EU test, once the test has been completed.

4 Red team providers

An intelligence-led red team test mimics the TTPs of real attackers on the basis of bespoke threat intelligence. In doing so, it looks to target the people, processes and technologies underpinning the CFs of an entity in order to test its protection, detection and response capabilities with no foreknowledge.

It allows the entity to understand its real-world resilience by stressing all elements of its business against the TTPs of the threat actors that are specific to its organisation. The intelligence-led red team test provides a comprehensive end-to-end understanding of weaknesses present in people, business processing, technology, and their associated intersection points, and provides a detailed threat assessment which can be used to further enhance the entity's situational awareness.

Intelligence-led red team tests differ from conventional penetration tests, which provide a detailed and useful assessment of technical and configuration vulnerabilities, often of a single system or environment in isolation. However, they do not assess the full scenario of a targeted attack against an entire entity (including the complete scope of its people, processes and technologies).

During the procurement process, entities must ensure that RT providers with the requisite skills are hired to perform intelligence-led red team tests, and these should not be confused with penetration testing services.

4.1 The role of RT provider

The RT provider plans and executes a TIBER-EU test of the target systems and services, which are agreed in the scope. This is followed by a review of the test and issues arising, culminating in a Red Team Test Report drafted by the RT provider.

The RT provider should expand on and execute the established threat scenarios identified by the TI provider and approved by the entity. The threat scenarios are developed from an attacker's point of view. The RT provider should indicate various creative options in each of the attack phases based on the various TTPs used by advanced attackers. This is in order to anticipate changing circumstances or is in case other attack methods do not succeed during the test. The scenario development is a creative process, and TTPs should not simply mimic scenarios seen in the past but should look to combine the TTPs of various relevant threat actors. The RT provider should aim to assess the cyber resilience posture of the entity in the light of the threat it faces.

The RT provider should follow a rigorous and ethical red team testing methodology, and should meet the minimum requirements defined in the TIBER-EU Framework, as set out below. The rules of engagement and specific testing requirements should be established by the RT provider and the entity.

The RT provider must demonstrate a willingness to work closely with the TI provider, which includes reviewing and commenting on the intelligence deliverables as well as transforming the threat scenarios into a cohesive and tractable Red Team Test Plan. Furthermore, the RT provider is expected to liaise and work with the TI provider throughout the testing in order to update the threat intelligence assessment and attack scenarios with relevant and up-to-date intelligence. Lastly, the RT provider is expected to work with the TI provider in order to design and deliver the final report issued to the entity.

4.2 RT provider requirements

To ensure that the RT provider is able to furnish the deliverables cited above in an effective and safe manner, it must display the highest standards. Consequently, the TIBER-EU Framework requires RT providers to meet specific requirements to also ensure that the test is recognised by the relevant authorities. The core requirements below are set to ensure that only the highest-quality providers, with sufficient experience and capabilities, can contribute to red team tests on the most critical functions of entities.

All TIBER-EU tests will require a red team, composed of a Red Team Test Manager and red team testers. A red team should comprise a mix of staff with a broad set of skills and experience, in areas such as red team testing, penetration testing, reconnaissance, threat intelligence, risk management, exploit development, physical penetration, social engineering and vulnerability analysis. The size of the red team will depend on the entity being tested, the scope of the test, and the specific skills and expertise required to deliver the test.

Table 3

RT Provider requirements to deliver TIBER-EU tests

Who	Requirements
RT provider (at company level)	At least five references from previous assignments related to intelligence-led red team tests Adequate indemnity insurance in place to cover activities which were not agreed upon in the contract and/or which stem from misconduct, negligence, etc.
Red Team Test Manager – responsible for the end-to-end management of the TIBER-EU red team test	Lead and oversight of the RT provider's activities for delivering a TIBER-EU test are ensured by a Red Team Test Manager Sufficient experience of the Red Team Test Manager in red team testing. Expectation: at least five years of experience in red team testing, including three years managing intelligence-led red team tests in the financial services industry Up-to-date CV and at least three references of the Red Team Test Manager from previous assignments to be provided to the entity, specifically in red team testing activities Background checks on the Red Team Test Manager by the RT provider (as a minimum). Enhanced background checks are conducted as required by the national authorities The Red Team Test Manager must have appropriate recognised qualifications and certifications (as set out in Annex 1)
Red team (all members of the team, except for the Red Team Test Manager) – responsible for conducting the TIBER-EU red team test	Sufficient experience of the red team members. Expectation for each member: at least two years of experience in red team testing Up-to-date CV for each member of the team to be provided to the entity Multi-disciplinary composition of the red team, with a broad range of knowledge and skills, such as: business knowledge, red team testing, penetration testing, reconnaissance, threat intelligence, risk management, exploit development, physical penetration, social engineering, vulnerability analysis and combinations thereof Background checks on each member of the red team are conducted by the RT provider (as a minimum). Enhanced background checks are conducted as required by the national authorities The red team members should have appropriate recognised qualifications and certifications (as set out in Annex 1)

It is the responsibility of the entity to ensure that the RT providers meet these requirements prior to formalising any test, and therefore it should undertake thorough due diligence during its procurement process.

However, it is recommended that the entity delegate this responsibility to accreditation and certification bodies in the EU. As soon as there is sufficient capability in the EU to conduct TIBER-EU accreditation and certification of RT providers and their staff, respectively, the entity should opt for only TIBER-EU accredited and certified RT providers[9]. The Services Procurement Guidelines will be updated by the TIBER-EU Knowledge Centre when such capability is deemed to be in place.

4.3 Guiding principles and criteria for selecting RT providers

When an entity decides to undertake a TIBER-EU test, one of the most significant decisions will be its selection of the RT provider. Given the sensitivity of the test, it is critical that the entity makes an informed decision about its procurement, ensuring that the highest-quality RT provider, which possesses the requisite skills, resources and capabilities to deliver a red team test, is chosen.

9 The accreditation and certification provider validates the baseline level of proficiency of the RT provider and its staff to provide red team testing services.

This section sets out the guiding principles and criteria for the entity to consider during its procurement process and when evaluating the capabilities of an RT provider. These principles are of a more qualitative nature than the requirements set out in Section 4.2, and thus entities should look to integrate these principles and criteria in their request for proposals and bilateral discussions with prospective providers, aided by the questions in Annex 3.

RT provider's reputation, history and ethics

Three of the most important criteria for a buyer of red team testing services are the reputation and history of the RT provider and the ethical conduct it both adopts and enforces.

A suitable and reputable RT provider should be able to clearly demonstrate its knowledge and expertise in red team testing. This should be focused on highlighting areas where risk to the entity can be minimised – such as understanding the legal and ethical challenges, and how their processes and methodologies will deliver results, whilst taking a risk-based approach.

Mature and capable RT providers are generally those that have conducted multiple assignments already for a broad range of entities in different jurisdictions; have first-hand experience of the issues and complexities involved; have a good depth and breadth of experience and knowledge of the financial services industry; and have appropriate processes and capabilities to conduct tests on a variety of critical functions and information systems.

Governance, security and risk management

It is important that the RT provider gives a high priority to governance, security and risk management. A competent RT provider should be able to provide assurances that the security of and risks associated with the entity's critical systems and confidential information (together with any other business risks) will be adequately addressed. The RT provider should be able to ensure that the results of its tests are generated, reported, stored, communicated, redacted (if necessary) and destroyed in a manner that does not put entities at risk.

During any red team test, it is likely that the red team will encounter sensitive or business-critical data related to the entity or its third party suppliers. The entity should ensure that the RT provider fully understands the sensitivity of this, and should put in place all the appropriate security objectives, policies and procedures to address these possible situations, including for data of the entities' third party suppliers which are in the scope of a TIBER-EU test. Overall, the entity will need to be comfortable that it can trust the RT provider and its individual testers.

Suitable and mature RT providers should have a robust ISMS with a bespoke security control framework and appropriate certification, based on recognised international standards. Examples of such certifications are included in Annex 1. The

ISMS should define a clear governance structure and processes, which are effectively established, implemented, operated, continuously monitored, tested, reviewed, maintained and improved.

The entity should request the RT provider to furnish evidence of its relevant internal information security policies that ensure the security and resilience of its services and methods. The entity should analyse these pieces of evidence, ensuring that they are aligned with the RT provider's high-level security objectives.

Methodology

RT providers should have robust methodologies in place to conduct the most advanced and innovative forms of red team testing. The RT provider should aspire to conduct the highest-level tests, such that they can mimic a nation state actor and demonstrate sophistication, agility, use of advanced techniques and perseverance to match the level of defence of an entity. The RT provider should have processes in place to be able to clearly explain its methodologies, how they evolve and how they result in effective and high-quality red team tests.

Staff competence

Staff employed by an RT provider should have deep technical capabilities in the specific areas that are relevant to the entity's target environment (e.g. web applications, infrastructure, mainframe, mobile or vendor-specific), as well as a contextual understanding of the business processes delivered by the entity. Given the unique nature of entities in the financial sector, the RT provider should have staff that possess the requisite experience and knowledge of conducting red team tests on such entities.

The RT provider should have staff members that are appropriately qualified and certified; such qualifications and certifications should not be confined to commonly accepted IT security certifications, but should include a combination of various types of qualifications and certifications, which enables the RT provider to conduct red team tests of the highest standard, using several methodologies and different TTPs. To obtain assurance that the red team has the requisite skills, there are a number of professional qualifications and certifications on the market, some of which have been set out in Annex 1. The RT provider should be able to demonstrate that its staff possess a blend of different skill-sets and specialisms. However, the entity should not rely on qualifications and certifications alone; rather, the entity should try to actively engage with the RT provider during the procurement process to gain an insight into the actual knowledge and experience of its staff.

R&D capability

Good indicators of RT providers' technology competency are the quality and depth of their technical R&D capability. Some RT providers will constantly develop specific methodologies to address different environments, such as infrastructure, mainframe, web applications, wireless, mobile, etc.

Collaborative working

The end-to-end TIBER-EU test requires a collaborative, transparent and flexible working approach, observed by both TI and RT providers. An RT provider must demonstrate a willingness to work in this way. This might include reviewing and commenting on the TI provider's deliverables, or working with the TI provider to transform threat scenarios into a cohesive and tractable Red Team Test Plan. Entities may choose to procure from one provider that is capable of providing both TI and RT services; however, in such circumstances, the TI and RT services should be provided by separate teams within the organisation. The entity should explore with the prospective RT providers how they can demonstrate experience of working in a collaborative spirit with TI providers – whether within their own organisation or with another, external TI provider.

Language support

Given the multinational nature of entities and the possible implementation of TIBER-EU across different jurisdictions in the EU, the RT provider should have the capability to deliver tests, perform reconnaissance and produce reports in different languages. For example, a commonly used tactic is "spear phishing", which would require the use of the local language to be plausible. The entity should discuss the RT provider's capabilities and resources in this regard.

When the RT provider also offers TI services, the entity should ensure that the provider can cover a broad range of key languages used by most common threat actors, to avoid missing a significant proportion of key relevant information.

In national implementations of the TIBER-EU Framework, the entity may ask the RT provider for a test report written in the local language. However, in the case of cross-border entities where mutual recognition is being sought amongst various authorities, the RT provider should be able to deliver the report written in English.

Confidentiality

The RT provider should not use information acquired in the context of TIBER-EU for services provided to other parties. Therefore, TIBER-EU information can only be used for the purpose for which it was provided. Furthermore, due to the confidential nature of TIBER-EU tests, information must be protected against unintentional

disclosure. The RT provider needs to be able to provide assurances that the security and risks associated with the confidential nature of TIBER-EU tests are being adequately addressed, in accordance with jurisdictional regulations.

The RT provider should agree with the procuring entity the protocols to destroy all sensitive information related to the entity and the outputs from the TIBER-EU test, once the test has been completed.

5 Possible roles of authorities

As authorities may adopt TIBER-EU within their jurisdictions, they can have a key role in engaging with prospective TI/RT providers. As the market for threat intelligence and red teaming evolves, authorities and their respective TCTs can play a proactive role in identifying providers that meet the TIBER-EU requirements.

In some jurisdictions, authorities and TCTs may play an active role in catalysing accreditation and certification capabilities. Among others, the authority and TCT may opt to undertake the accreditation and certification process themselves, or they may liaise with industry bodies in the jurisdiction that already undertake this task. In principle, an accreditation and certification provider would be expected to validate the baseline level of proficiency of the TI and RT providers and their staff to deliver TIBER-EU tests.

In cases where there are no accreditation and certification providers, the authorities and TCTs may work with entities and TI/RT providers to develop or enhance self-assessment templates, which can be used by TI/RT providers to demonstrate their capabilities to deliver TIBER-EU tests. Alternatively, authorities and TCTs may explore other tools to help ease the process of ensuring that entities can source the appropriately qualified TI/RT providers to deliver TIBER-EU tests.

Authorities and TCTs may act as a central point of contact for entities and TI/RT providers, connecting them to each other, to facilitate the procurement process.

Authorities and TCTs can make an assessment of the level of maturity of the TI and RT market within their respective jurisdiction, gather more experience with the issue of accreditation and certification and liaise with the TIBER-EU Knowledge Centre to assess whether the Guidelines should be updated.

6 Annexes

6.1 List of qualifications and certifications *(last updated: June 2020)*

The following is a detailed, though not exhaustive, list of qualifications and certifications available in the market for TI and RT practitioners and organisations. Providers should demonstrate that their staff possess a broad range of such qualifications and certifications, and at an organisational level that they are suitably certified in security management. It should be noted that this list provides indicators and benchmarks that entities may leverage for their own assessment of procuring these security services, and entities should apply their professional judgement during the due diligence process and liaise with the respective TCT for further guidance (if necessary). The list provides a snapshot of the most well-known qualifications and certifications at international level and may be updated when there are major changes to Guidelines.

TI and RT managers

Certification body/Standard setting body	Qualification
CREST	CREST Certified Threat Intelligence Manager (CCTIM)
CREST	CREST Certified Simulated Attack Manager (CCSAM)
Offensive Security	Offensive Security Certified Expert (OSCE)
eLearnSecurity	eLearnSecurity Certified Penetration Tester eXtreme (eCPTX)

TI and RT teams

Certification body/Standard setting body	Qualification
CREST	CREST Certified Simulated Attack Specialist (CCSAS)
ISACA	CSX Penetration & Vulnerability Tester Pathway
	CSX-P - Cybersecurity Practitioner Certification
(ISC)2	Certified Information Systems Security Professional (CISSP)
	Systems Security Certified Practitioner (SSCP)
SANS Institute - GIAC	GIAC Penetration Tester (GPEN)
	GIAC Web Application Penetration Tester (GWAPT)
	GIAC Exploit Researcher and Advanced Penetration Tester (GXPN)
	GIAC Mobile Device Security Analyst (GMOB)
	GIAC Assessing and Auditing Wireless Networks (GAWN)
Offensive Security	Offensive Security Certified Professional (OSCP)
	Offensive Security Wireless Professional (OSWP)
	Offensive Security Exploitation Expert (OSEE)
	Offensive Security Web Expert (OSWE)
eLearnSecurity	eCPPT e-learn Security Certified Professional Penetration Tester (eCPPT)
	eLearnSecurity Web Application Penetration Tester (eWPT)
	eLearnSecurity Web Application Penetration Tester eXtreme (eWPTX)
	eLearnSecurity Mobile Application Penetration Tester (eMAPT)
	eLearnSecurity Certified eXploit Developer (eCXD)
Others	EC-Council Certified Security Analyst (ECSA)
	Licensed Penetration Tester (LPT)
	Certified Ethical Hacker (CEH)

TI and RT providers

Certification body/Standard setting body	Qualification
ISO	ISO/IEC 27001, ISO/IEC 29147, ISO 30111
NIST	NIST 800-115 for Information Security
FedRAMP	FedRAMP-Compliant data centres
FIPS	FIPS 140-2-Compliant encryption for data protection

6.2 List of questions to facilitate the procurement process – TI providers

When the entity undertakes its procurement process and engages with potential providers, there are a number of questions it can pose to the prospective providers to gauge their levels of competence and suitability to deliver a TIBER-EU test. Although the entity (or an accreditation and certification provider) is responsible for validating the core requirements of the providers, as set out in the Guidelines, there are a number of questions of a more qualitative nature that the entity should pose to

determine the provider's eligibility. These questions are largely based on the guiding principles and criteria set out in the Guidelines.

The entity may use the questions below in its request for proposals, in the form of a self-assessment for the prospective provider to complete, or integrate them into its existing procurement processes and documents. Responses to the below questions will provide useful input to the entity (or accreditation and certification provider) in carrying out due diligence.

TI Providers

Reputation, history and ethics

Can the TI provider provide evidence of a solid reputation, history and ethics (e.g. a full trading history, a strong history of performance, good feedback from both clients and providers and a reliable financial record)?

More specifically, can the TI provider provide at least three reference from previous assignments related to red team tests?

Is the TI provider accredited by an accreditation/industry body in the European Union?

Does the TI provider adhere to a formal Code of Conduct and Ethical Framework?

Does the TI provider contribute to specialised industry events (such as those run by BlackHat or RSA Conferences, etc.)?

Is the TI provider sufficiently insured to conduct TIBER-EU tests? More specifically, does the TI provider have adequate indemnity insurance in place to cover activities which were not agreed upon in the contract and/or which stem from misconduct, negligence, etc?

What is the TI provider's recruitment policy and process?

Does the TI provider ensure that its staff members are adequately vetted?

Does the TI provider have adequate knowledge of the different jurisdictional regulations and requirements to conduct red team tests?

Governance, security and risk management

Are the TI provider's ISMS, and its implementation, independently audited? Can the TI provider share these audits with the entity?

Does the TI provider hold any international certifications, with specific regard to security and risk management?

Can the TI provider offer independent assurances that the risks associated with the red team test (including the entity's confidential information and any other business risks) will be adequately addressed and protected and compliance requirements met?

How does the TI provider ensure that the results of test are generated, reported, stored, and communicated, redacted (if necessary) and destroyed in a manner that does not put the entity at risk?

How does the TI provider ensure that no data leakage occurs from its staff's devices and teams?

Methodology

Does the TI provider have a clearly documented methodology for conducting threat intelligence and reconnaissance?

Does the TI provider have a comprehensive threat intelligence collection process and function, which provides the raw materials for conducting threat intelligence analysis?

Does the TI provider have access to threat intelligence from a broad range of sources?

Does the TI provider have the capability to analyse threat intelligence in multiple languages?

Does the TI provider have the capability to analyse different types of threat intelligence (e.g. OSINT, HUMINT, SIGINT, etc.)?

What mechanisms does the TI provider have in place to ensure that it can keep up to date with the latest tactics, techniques and procedures of advanced real-life attackers, and how are these transmitted to its staff?

Does the TI provider take into account public data about previous incidents that would be relevant to the threats today?

Does the TI provider take into account, and keep confidential, private data about previous incidents that would be relevant to the threats today?

Does the TI provider look at the short, medium and longer-term goals of the business that might provide information on the likely interests of a potentially hostile party?

Does the TI provider ask for previous risk assessments or risk models exercises?

Does the TI provider have a comprehensive view of the financial sector and does it understand the current geopolitical context the entity is operating in?

Staff competence

Does the TI provider employ a broad range of staff with varying expertise? Specifically, can the TI provider deliver services for TIBER-EU tests with teams, led by Threat Intelligence Managers?

Does the TI provider have Threat Intelligence Managers with at least five years of experience in threat intelligence, including three years producing threat intelligence in the financial services industry?

Do the Threat Intelligence Team members each have at least two years of experience in threat intelligence?

Can the TI provider demonstrate that its Threat Intelligence Team has experience in delivering threat intelligence for red team tests?

Can the TI provider specify named individuals who will be responsible for managing and conducting the test, their experience of the environment within the scope, their qualifications and the exact role each individual will perform?

Can the TI provider demonstrate that its Threat Intelligence Team is multi-disciplinary, with a broad range of skills including OSINT, HUMINT and geopolitical knowledge?

Can the Threat Intelligence Manager provide an up-to-date CV and at least three references from previous assignments, specifically in delivering threat intelligence for red team testing activities?

Can the TI provider provide an up-to-date CV for each member of the Threat Intelligence Team?

What qualifications do the TI provider's staff hold in the various areas in which tests may be required?

What continuous professional development programme does the provider have in place to ensure that its staff continuously enhance their skills?

Are all staff experienced in the specific dynamics of the financial services industry?

6.3 List of questions to facilitate the procurement process – RT providers

RT Providers

Reputation, history and ethics

Can the RT provider provide evidence of a solid reputation, history and ethics (e.g. a full trading history, a strong history of performance, good feedback from both clients and providers and a reliable financial record)?

More specifically, can the RT provider provide at least five references from previous assignments related to red team tests?

Is the RT provider accredited by an accreditation/industry body in the European Union?

Does the RT provider adhere to a formal Code of Conduct and Ethical Framework?

Does the RT provider contribute to specialised industry events (such as those run by BlackHat or RSA Conferences, etc.)?

Is the RT provider sufficiently insured to conduct TIBER-EU tests? More specifically, does the RT provider have adequate indemnity insurance in place to cover activities which were not agreed upon in the contract and/or which stem from misconduct, negligence, etc?

What is the RT provider's recruitment policy and process?

Does the RT provider ensure that its staff members are adequately vetted?

Does the RT provider have adequate knowledge of the different jurisdictional regulations and requirements to conduct red team tests?

Governance, security and risk management

Are the RT provider's ISMS, and its implementation, independently audited? Can the RT provider share these audits with the entity?

Does the RT provider hold any international certifications, with specific regard to security and risk management?

Does the RT provider apply independently validated security and risk management controls during the red team testing process?

Can the RT provider offer independent assurances that the risks associated with the red team test (including the entity's confidential information and any other business

risks) will be adequately addressed and protected and compliance requirements met?

How does the RT provider ensure that the results of test are generated, reported, stored, communicated, redacted (if necessary) and destroyed in a manner that does not put the entity at risk?

Does the RT provider record and log all tests carried out by its testers, and what is the retention period of these records and logs?

How does the RT provider ensure that no data leakage occurs from its staff's devices and systems?

Methodology

Has the RT provider ever performed testing that emulates the most advanced attackers involving people, processes and technical weaknesses? Can the RT provider give examples and references?

Is the RT provider able to demonstrate exploits or vulnerabilities it has found in other similar environments?

Is the RT provider adequately capable of collecting threat intelligence concerning its (potential) trargets?

Does the RT provider have experience emulating advanced attacks on live critical core financial systems? If yes, the entity should request evidence.

Is the RT provider mature and capable enough to adapt its attack scenarios and techniques during the test, dependent on the behaviour of the target?

Can the RT provider provide evidence that it can provide high-quality services, including the methodologies, tools, techniques and sources of information it will use as part of the testing process?

Is the RT provider mature and creative enough to develop high-end scenarios using cutting-edge techniques available on the market? Does the RT provider have knowledge of the latest vulnerabilities and can it develop its own tools?

Does the RT provider have knowledge and experience of the financial sector and the functioning of its systems?

How does the RT provider perform rigorous and effective team tests to ensure that a wide range of system attacks is simulated?

Can the RT provider describe its proven testing methodology that is tailored for particular types of environment (e.g. infrastructure, web applications and mobile computing)?

Can the RT provider demonstrate its red team testing capabilities (e.g. by making a presentation, showing examples of similar projects it has undertaken) and provide a sample report?

Does the RT provider have independently reviewed quality assurance processes that it applies to each test, in order to ensure client requirements are being met in a secure and productive manner?

What is the exploitation process used by the RT provider? How does the RT provider ensure that it is safe?

Can the RT provider support out of business hours testing?

What is the RT provider's peak testing capacity?

Can the RT provider's infrastructure and team support the peak requirement of the entity?

Staff competence

Does the RT provider employ a broad range of staff with varying expertise? Specifically, can the RT provider deliver services for TIBER-EU tests with teams, led by Red Team Test Managers?

Does the RT provider have Red Team Test Managers with at least five years of experience in red team testing, including three years managing red team tests in the financial services industry?

Do the red team members each have at least two years of experience in red team testing?

Can the RT provider specify named individuals who will be responsible for managing and conducting the test, their experience of the environment within the scope, their qualifications and the exact role each individual will perform?

Can the RT provider demonstrate that the composition of its red teams is multi-disciplinary, with a broad range of knowledge and skills, such as: business knowledge, red team testing, penetration testing, reconnaissance, threat intelligence, risk management, exploit development, physical penetration, social engineering, vulnerability analysis and combinations thereof?

Can the Red Team Test Manager provide an up-to-date CV and at least three references from previous assignments, specifically in red team testing activities?

Can the TI provider provide an up-to-date CV for each member of the red team that will conduct the TIBER-EU test?

What qualifications do the RT provider's staff hold in the various areas in which tests may be required?

What continuous professional development programme does the provider have in place to ensure that its staff continuously enhance their skills?

Are all staff experienced in the specific dynamics of the financial services industry?

How do the RT provider's testers identify "root cause" findings, strategically analyse findings in business terms, help to develop security improvement strategies and recommend counter measures to both address vulnerabilities and prevent them from recurring?

R&D capability

Does the RT provider have an active, continuous and relevant R&D capability?

Has the RT provider produced research papers, published vulnerabilities or won awards in the industry?

Does the RT provider perform sufficient R&D to be able to identify all significant vulnerabilities?

How does the RT provider carry out specially tailored, manual tests to help detect unknown vulnerabilities, rather than simply using a standard of set tools?

Does the RT provider have proprietary tools and technology?

6.4 TI provider agreement checklist

When formalising the arrangements for a TIBER-EU test, the entity and TI provider could agree on the following clauses as part of their agreement. The agreement must be shared with the TIBER Test Manager.

Table 4

Example of TI provider agreement checklist

Clause	√
Intellectual property	
The contract includes agreements on intellectual property (IP), stating that IP remains with the entitled party.	
Non-disclosure agreement	
The contract has a non-disclosure agreement, stating as a minimum that: • information will not be used outside of the context of TIBER-EU • information will only be used for the purpose for which it was provided/collected; and • the TI provider must ensure that all staff involved in the service (including staff provided by external parties) adhere to the agreements made concerning security and confidentiality.	
Sharing threat intelligence information	
The threat intelligence report that the entity receives is the property of the entity. The entity therefore has the right to share this information with other relevant parties. The TI provider cannot share this information with any other party without the prior approval of the entity.	
Information security	
The TI provider demonstrates its security measures and procedures and how these operate. For example: • the TI provider has a security policy, approved by its Board of Directors; • the TI provider has a demonstrable effective Information Security Management System; • information security is an integral part of the TI provider's risk management processes; • every risk-mitigating measure, including those regarding information security, is documented and reviewed regularly; • information systems used for storing and processing information regarding the entity are adequately protected and secured using state of the art methods, including periodical penetration tests and vulnerability assessments; • information asset management is in place including inventories, retention and secure deletion and destruction; and • all information related to TIBER-EU is accessed on a need to know basis. This is controlled by a combination of pro-cedural and technical measures, and all access to this information is logged and monitored.	
Acceptance of provided services	
The entity and the TI provider define criteria and validation methods according to which the delivered services will be accepted by the entity.	
Pricing	
Pricing is part of the agreement. The TI provider is transparent in the pricing of its services, including any additional or value added services.	
Continuity	
The TI provider has implemented policies and procedures to ensure continuity of its services during the term of the contract.	
Audit	
The TI provider gives the entity permission to verify the process and the results of the agreement by means of an (external) audit. The agreement specifies by which party, at what time, at what cost (including the distribution of costs amongst the contracting parties) and against which audit standards.	
Assurance	
The TI provider can provide assurance, via its second and third lines of defence or via external assurance providers, that its risk management objectives related to the service are met. The TI provider shows that processes crucial to the service and continuity are effective.	
Legal privacy requirement (data transfer agreement)	
If processing (including storing) of data takes place outside the legal premises of the European Economic Area (EU + Switzerland, Norway and Iceland), a data transfer agreement confirming compliance with EU standards is required. This requirement is also effective when data are processed in the European Economic Area but are accessible for e.g. technical support from within countries outside the European Economic Area.	
Legal privacy requirement (personally identifiable information)	
If the TI provider processes personally identifiable information, it will do so according to the GDPR.	
Service quality	
The TI provider provides services in accordance with the quality associated with the TIBER-EU standards. The agreed quality standards, as well as related technical and operational security requirements, are defined in a service level agreement between the TI provider and the entity. Additional requirements (e.g. SLAs and KPIs) can be added by the procurement staff of the entity.	

Security incidents and risks
Security incidents regarding the agreed upon services are always reported immediately to the entity. The TI provider has implemented an efficient process to ensure the timely notification of security incidents and risks related to the services provided to the entity. When asked, the TI provider is willing to provide the entity with the details of this process.
Responsible disclosure procedure (RDP)
The TI provider and entity should agree that: • if the TI provider finds vulnerabilities or other weaknesses during the research on an entity, it will disclose these to the white team of that entity; and • if the TI provider finds vulnerabilities or other weaknesses during the research on an entity that relate to a product that is generally used, e.g. in operating systems, it will disclose these vulnerabilities or weaknesses to the vendor of that particular product.
Screening of employees
The TI provider has an adequate process for assuring that its employees are of outstanding reputation, are not and were never involved in criminal activity relevant to his or her current occupation and have sufficient skills to perform TI tasks for entities. The TI provider is willing to demonstrate the existence and the operation of this process.
Change of services
The entity or its affiliates are always entitled to ask for a change in the way the TI provider provides its services to the entity.
Exit clause (general)
The TI provider provides formal procedures to assure the destruction of any threat intelligence regarding the entity after the end of the contract and relationship between the TI provider and the entity.
Exit clause (confidentiality)
Arrangements regarding confidentiality are still valid after the end of the contract and relationship between the TI provider and the entity.

6.5 RT provider agreement checklist

When formalising the arrangements for a TIBER-EU test, the entity and RT provider could agree on the following clauses as part of their agreement. The agreement must be shared with the TIBER Test Manager.

Table 5

Example of RT provider agreement checklist

Clause	√
Intellectual property	
The contract includes agreements on intellectual property (IP), stating that IP remains with the entitled party.	
Non-disclosure agreement	
The contract has a non-disclosure agreement, stating as a minimum that: • information will not be used outside of the context of TIBER-EU; • information will only be used for the purpose for which it was provided/collected; and • the RT provider must ensure that all staff involved in the service (including staff provided by external parties) adhere to the agreements made concerning security and confidentiality.	
Sharing threat-intelligence information	
The threat intelligence report that the entity receives is the property of the entity. The entity therefore has the right to share this information with other relevant parties. The RT provider cannot share this information with any other party without the prior approval of the entity.	
Roles and responsibilities	
The contract defines and states roles and responsibilities to avoid confusion, misunderstanding or abuses. One person within the RT provider should be accountable during the whole contract life cycle to ensure that: • security risks and requirements are fully understood; • appropriate processes are in place and a minimum acceptable level of residual risk is agreed with the entity and duly accepted by each party; • security risks are managed and appropriate processes are in place and communicated to the entity; • appropriate support is provided to the entity; and • contractual clauses are respected.	
Information security	
The RT provider demonstrates its security measures and procedures and how these operate. For example: • the RT provider has a security policy, approved by its Board of Directors; • the RT provider has a demonstrable effective Information Security Management System; • information security is an integral part of the RT provider's risk management processes; • the RT provider should provide evidence of its relevant internal information security policies ensuring the security and resilience of its products and services; • every risk-mitigating measure, including those regarding information security, is documented and reviewed regularly; • information systems used for storing and processing information regarding the entity are adequately protected and secured using state of the art methods, including periodical penetration tests and vulnerability assessments; • information asset management is in place including inventories, retention and secure deletion and destruction; and • all information related to TIBER-EU is accessed on a need to know basis. This is controlled by a combination of procedural and technical measures, and all access to this information is logged and monitored.	
Service quality	
The RT provider ensures services in accordance with the quality associated with the TIBER-EU standards. The agreed quality standards, as well as related technical and operational security requirements, are defined in a service level agreement between the RT provider and entity. These high-level requirements aim to provide the control required to mimic the most advanced attacks on live critical systems. Additional requirements (e.g. SLAs and KPIs) can be added by the procurement staff of the entity.	
Acceptance of provided services	
The entity and the RT provider define criteria and validation methods according to which the delivered services will be accepted by the entity.	
Pricing	
Pricing is part of the agreement. The RT provider is transparent in the pricing of its services, including any additional or value added services.	
Continuity	
The RT provider has implemented policies and procedures to ensure continuity of its services during the term of the contract.	
Audit	
The RT provider gives the entity permission to verify the process and the results of the agreement by means of an (external) audit. The agreement specifies by which party, at what time, at what cost (including the distribution of costs amongst the contracting parties) and against which audit standards.	
Assurance	

The RT provider can provide assurance, via its second and third lines of defence or via external assurance providers, that its risk management objectives related to the service are met. The RT provider shows that processes crucial to the service and continuity are effective.

Legal privacy requirements (data transfer agreement)

If processing (including storing) of data takes place outside the legal premises of the European Economic Area (EU + Switzerland, Norway and Iceland), a data transfer agreement confirming compliance with EU standards is required. This requirement is also effective when data are processed in the European Economic Area but are accessible for e.g. technical support from within countries outside the European Economic Area.

Legal privacy requirement (personally identifiable information)

If the RT provider processes personally identifiable information, it will do so according to the GDPR.

Security incidents and risks

Security incidents regarding the agreed upon services are always reported immediately to the entity.

The RT provider has implemented an efficient process to ensure the timely notification of security incidents and risks related to the services provided to the entity. When asked, the RT provider is willing to provide the entity with the details of this process.

Reporting of vulnerabilities and weaknesses

The RT provider and the entity agree that:

- if the RT provider finds vulnerabilities or other weaknesses during the research on an entity, it will disclose these to the white team of that entity; and
- if the RT provider finds vulnerabilities or other weaknesses during the research on an entity that relate to a product that is generally used, e.g. in operating systems, it will disclose these vulnerabilities or weaknesses to the vendor of that particular product.

Screening of employees

The RT provider has an adequate process for assuring that its employees are of outstanding reputation, are not and were never involved in criminal activity relevant to his or her current occupation and have sufficient skills to perform intelligence tasks for entities. The RT provider is willing to demonstrate the existence and the operation of this process.

Credentials of the RT provider's employees should be provided to demonstrate their relevant experience.

Employees' security knowledge and training

The RT provider should provide sufficient evidence regarding the training programme of its employees.

The entity should request the RT provider to perform and provide its due diligence to ensure that its employees have sufficient security and technical knowledge, skills and qualifications to avoid any unintentional alterations of the entity's systems. This due diligence should demonstrate that its red team meets the requirements set out in the Services Procurement Guidelines.

Personnel changes

All personnel from the RT provider or downstream sub-contractors, who are involved in the entity's TIBER-EU test, should sign a confidentiality and non-disclosure agreement. The contract between the entity and the RT provider should include clauses regarding confidentiality and personal data protection.

Any change or replacement of personnel in the scope of the test should be agreed with the entity.

Change of services

The entity or its affiliates are always entitled to ask for a change in the way the RT provider provides its services to the entity.

Exit clause (confidentiality)

Arrangements regarding confidentiality are still valid after the end of the contract and relationship between the RT provider and the entity.

Exit clause (general)

The RT provider provides formal procedures to assure the destruction of any information security-related information regarding the entity after the end of the contract and relationship between the RT provider and the entity.

Postal address 60640 Frankfurt am Main, Germany
Telephone +49 69 1344 0
Website www.ecb.europa.eu

For terminology and abbreviations, please refer to the ECB glossary.