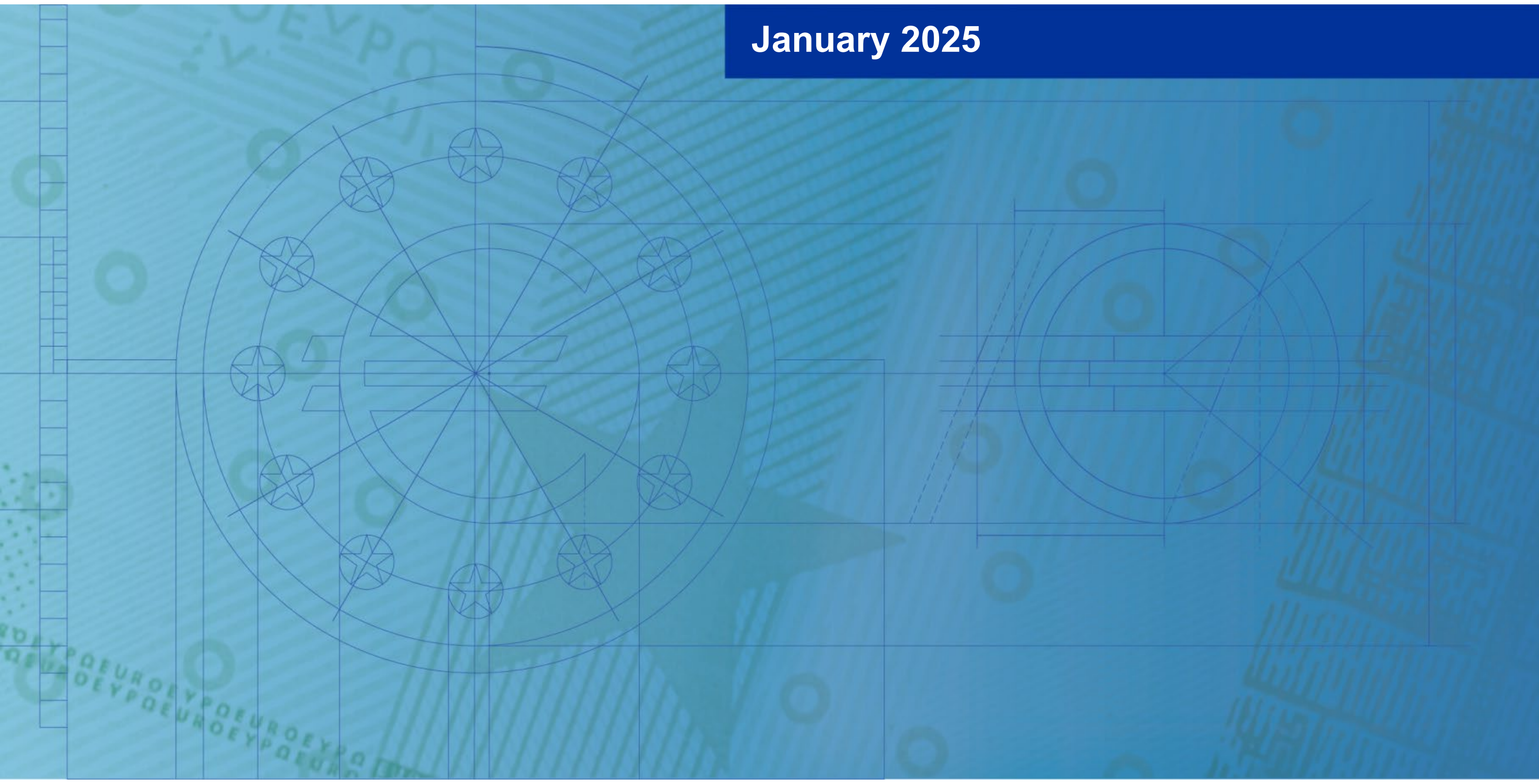
EUROPEAN CENTRAL BANK
EUROSYSTEM

TIBER-EU

Guidance for Service Provider Procurement



January 2025

Contents

1 Introduction

The Threat Intelligence Provider (TIP) and the Red Team Testers (RTT) are executing the main reconnaissance and testing activities and are therefore at the core of each TIBER test. Since a TIBER test is conducted on live production systems, only TIPs and RTT of the highest quality shall be procured by the Control Team (CT) to ensure a safe, realistic and high-quality test.

1.1 Purpose of this document

The purpose of this document is to provide the relevant stakeholders with information on the requirements[1] for procuring the TIP and RTT. It also aims at providing guidance on important aspects to be considered during these efforts. In this document, RTT is the generic term for the testers and is used for both internal and external testers. The term ‘RT provider’ is used in the context of contractual agreements, requirements or questions regarding the provider on a company/group level.

1.2 Target Audience

This TIBER-EU Guidance for Service Provider Procurement is mainly aimed at the CT procuring a TIP as well as RTT in the scope of a TIBER test. It is also aimed at TIPs and RTT offering their services to financial entities for conducting TIBER tests. Beyond that, it is useful to read for all stakeholder of a TIBER engagement involved or interested in the TIBER procurement process.

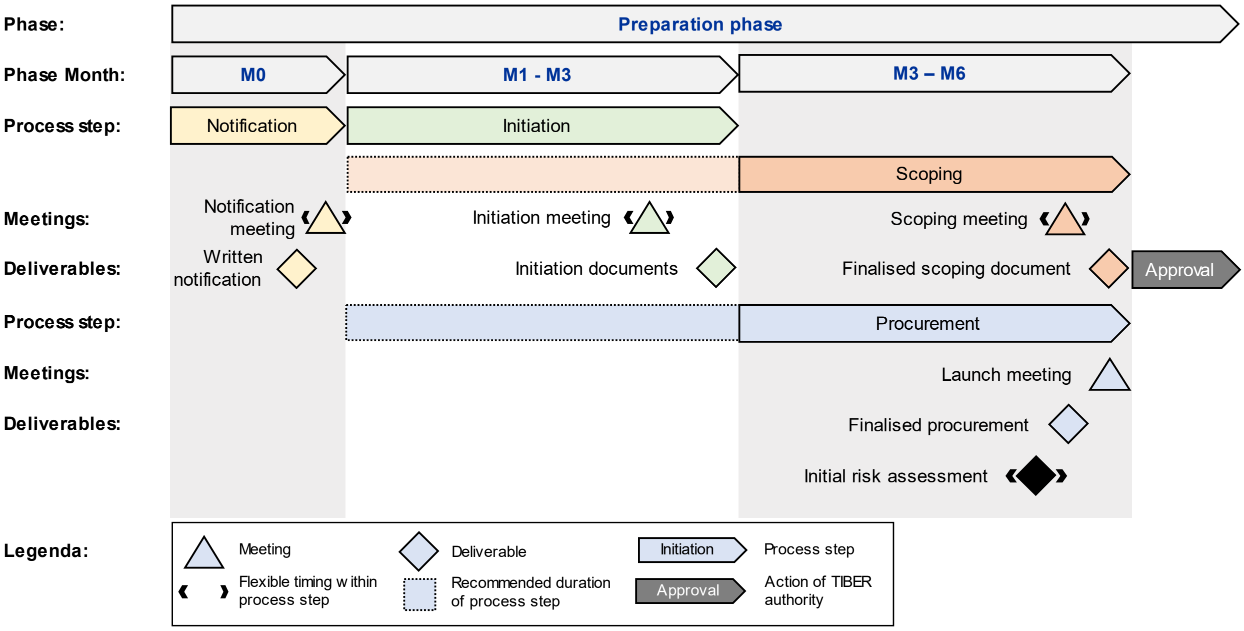
1.3 Location within testing process

The TIP and RTT are procured by the CT during the procurement process step of the preparation phase. Further details on the TIBER-EU process can be found in the TIBER-EU framework.

[1] In addition to the minimum requirements for complying with the TLPT obligations under DORA, this document also includes operational TIBER-EU guidance based on best practices, knowledge and experience from numerous previous tests.

Figure 1[2]

The procurement process step in the preparation phase



[2] Note that only the actions of the TIBER authority are included in the figure that have an impact on the timelines of the test. The figure is not an exhaustive overview of all actions to be undertaken by the involved stakeholders.

2 Requirements for procuring service providers

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

In exceptional circumstances, and only after discussing with the Test Manager (TM), the entity may contract a TIP and RTT that do not meet some of the minimum requirements for providers, as set out in this document. In this case, the entity has to adopt appropriate measures mitigating the risks relating to the lack of compliance with the requirements, and provide evidence of these measures established to the TM. The CT must not proceed with contracting the selected TIP and RTT if the TM assesses that the selected TIP and RTT do not ensure compliance with the applicable standards and requirements. It is therefore strongly advised for the CT to liaise with the TM in due time. The TM will not give commercial advice on the provider selection.

2.1 TIP requirements

All TIBER-EU tests requires a Threat Intelligence Team, composed of a Threat Intelligence Manager and a minimum of one additional Threat Intelligence Team member.

Table 1
TIP requirements to deliver TIBER-EU tests

Who	Requirements
TI Provider (at company level)	• Provides at least three references from previous assignments in the context of threat intelligence for penetration testing and red team testing. • Provides copies of certifications that are appropriate according to recognised market standards for the performance of their activities. • The provider is duly and fully covered by relevant professional indemnity insurances, including against risks of misconduct and negligence. • Capacity to form a TI team of at least one manager and one additional member, with adequate replacement available if needed. • No previous or current services delivered for the entity that would present a conflict of interest with respect to the financial entity, ICT third-party service provider or an ICT intra-group service provider involved in the TIBER test.
Threat Intelligence Team (all members of the team)	• Shall include a broad range and appropriate level of professional knowledge and skills including intelligence gathering tactics (e.g. HUMINT, OSINT), techniques and procedures, geopolitical, technical and sectorial knowledge as well as adequate communication and project management skills to clearly present and report on the current status, next steps and result of the engagement at any point during the test. • Are able to explain advanced, technical TI subjects to technical experts (i.e. members of the Blue Team) and to non-experts in an understandable manner, delivering actionable threat intelligence for the institution. • Up-to-date CV for each member of the team to be provided to the entity. • The two core members need to have a combined participation in at least three previous different assignments in delivering threat intelligence in the context of penetration testing and red team testing. • The team should have appropriate recognised qualifications and certifications for threat intelligence. • Not simultaneously perform any blue team tasks or other services that may present a conflict of interest with respect to the financial entity, ICT third-party service provider or an ICT intra-group service provider involved in a TIBER test to which they are assigned. • Be separated from, and not reporting to, staff of the same provider providing the Red Team Testers for the same TIBER test.
Threat Intelligence Manager – responsible for the end-to-end management of the threat intelligence for a TIBER-EU test	• At least five years of experience in threat intelligence.
Threat Intelligence Team, except for the Threat Intelligence Manager	• At least two years of experience in threat intelligence.

2.2 RTT requirements

All TIBER-EU tests will require a Red Team, composed of a Red Team Test Manager and a minimum of two Red Team Testers.

Table 2
RT Testers requirements to deliver TIBER-EU tests

Who	Requirements
RT provider (at company/group level)	Provides at least five references from previous assignments in the context of penetration testing and red team testing. Provides copies of certifications that are appropriate according to recognised market standards for the performance of their activities. The provider is duly and fully covered by relevant professional indemnity insurances, including against risks of misconduct and negligence. Capacity to form a Red Team of at least three persons, with adequate replacement available if needed, also to handle unforeseen events or for specific technologies/situations. No previous or current services delivered for the entity that would present a conflict of interest with respect to the financial entity, ICT third-party service provider or an ICT intra-group service provider involved in the TIBER test.
Red Team (all members of the team)	Shall include a broad range and appropriate level of professional knowledge and skills, such as: knowledge about the business of the financial entity, red team testing, penetration testing, reconnaissance, threat intelligence, risk management, exploit development, physical penetration, social engineering, vulnerability analysis, as well as adequate communication and project management skills to clearly present and report on the current status, next steps and the result of the engagement at any point during the test. Are able to explain advanced, technical RT-subjects to both technical personnel (such as the members of the BT) and to non-experts in an understandable manner, guiding the CT through the RT phase in a clear manner. Up-to-date CV for each member of the team to be provided to the entity. Should have appropriate recognised qualifications and certifications. The three core team members need to have a combined participation in at least five previous assignments related to penetration testing and red team testing. Not be employed by, nor provide services to, a provider that simultaneously performs blue team tasks for a financial entity, ICT third-party service provider or an ICT intra-group service provider involved in the same TIBER test. Be separated from any staff of the same provider simultaneously providing threat-intelligence services for the same TIBER test.
Red Team Test Manager – responsible for the end-to-end management of the TIBER-EU red team test	At least five years of experience in penetration testing and red team testing.
Red team members, except for the Red Team Test Manager	At least two years of experience in penetration testing and red team testing.

3 Considerations when procuring service providers

3.1 General considerations

As entities go through the procurement process, they are encouraged to seek further clarification with the TM regarding the selection criteria, TIP and RTT 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 TIP/RTT, allowing the entities to gain a deeper understanding of the TIP/RTT capabilities.

As the market for threat intelligence and red team testing varies widely, it is recommended that entities, the TCTs, and the TIP/RTT, collaborate closely to ensure a standardised and consistent approach in using the TIP/RTT services. This also ensures a common understanding of the standards required to perform TIBER tests.

3.1.1 Team size and availability

The size of the teams will depend on the entity being tested, the scope of the test, and the specific skills and expertise required to deliver the test. Without prejudice to the above-mentioned minimum criteria, adequate staffing of both the TIP as well as the RTT is important.

Also, small provider teams are at risk of falling short of resourcing, e.g. during holiday periods, leave or other absence. Therefore, the entity should pay attention to personnel turnover when selecting a provider. A TIBER test takes several months, and key people play an important role for the success of the test. Frequent turnover in a team may impact the test negatively. Any changes in the composition of the TIP or RTT must be communicated and agreed by the CTL and TM.

3.1.2 Reputation, history and ethics

Three of the most important criteria for a buyer of threat intelligence or red team services are i) the reputation, ii) history of the provider and iii) the ethical conduct it both adopts and enforces. Trustworthiness is the underlying principle of these key elements. Without trustworthiness of the reputation, history and ethics of a provider have little value.

A suitable and reputable TIP/RTT should be able to clearly demonstrate its knowledge and expertise in the services they provide, especially 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, and how their processes and methodologies will deliver results, whilst taking a risk-based approach.

Mature and capable 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 either gather, analyse and produce threat intelligence on a variety of entities or to conduct tests on critical or important functions (CIFs) and information systems.

3.1.3 Governance, security and risk management

Conducting a TIBER-EU test entails certain risks for all involved due to the vital nature of the operational systems, personnel, and procedures engaged in the testing. There's a risk of triggering service disruptions, unforeseen system failures, harm to essential operational systems, or compromising data integrity, including issues with data privacy and the management and storage of sensitive information. These risks underscore the necessity for proactive and stringent risk management. The TIBER-EU framework accordingly places significant emphasis on the implementation of strong risk management measures during the test's entire duration to guarantee its safe execution.

To ensure a controlled and safe test, one prescribed control is the use of specialist external TIP and RTT, 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.

It is important that the provider gives a high priority to governance, security and risk management. A competent 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 provider should be able to ensure that the results of its intel gathering or testing activities 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 TIP/RTT will encounter sensitive or business-critical data related to the entity or its third-party suppliers. The entity should ensure that the TIP/RTT fully understand 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 TIP/RTT.

Suitable and mature providers should have a robust Information Security Management System (ISMS) with a bespoke security control framework and appropriate certification, based on recognised international standards. 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 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 provider's high-level security objectives.

3.1.4 Multi-framework test

While this document details the protocols for TIPs and RTT within the EU to carry out TIBER-EU tests, global organizations might be required to perform these tests outside the EU or in conjunction with non-EU authorities that have their own versions of red team testing frameworks. Under these conditions, it's crucial for the organizations to grasp the regulations of the relevant authorities in other jurisdictions. Moreover, they should actively compare the different regulatory demands. This becomes especially critical when an organization intends to leverage test outcomes to fulfil the criteria of foreign regulatory bodies. In such instances, the organization must engage with all pertinent authorities, which may offer advice on procurement stipulations. For instance, certain jurisdictions may require proof of expertise through recognized accreditation and certification. Organizations are advised to ensure their strategy aligns with the expectations of all jurisdictions involved right from the planning phase. Regardless, the stipulations outlined in this document represent the foundational standards necessary for the acknowledgment of a TIBER-EU test.

3.1.5 Language support

Given the multinational nature of entities and the possible implementation of TIBER-EU across different jurisdictions in the EU, the providers should have the capability to deliver threat intelligence, perform reconnaissance, conduct testing activities, as well as presentations and reports in different languages. For example, reconnaissance might be collected in different languages, "spear phishing" shall be conducted in the respective language of the entity and presentations/reports should be delivered in a way it is consumable by the respective stakeholders. The entity should discuss the provider's capabilities and resources in this regard.

3.1.6 Service provider rotation

It is highly recommended to rotate service providers for every test. A new external service provider might bring new insights to the testing entity through a fresh outlook, other research routines, different methods and a different testing approach.

3.1.7 Impartiality of service providers

A service provider that is currently or has previously provided IT-services, cybersecurity services or cyber intelligence services to the entity, ICT third-party service provider or an ICT intra-group service provider involved in the TIBER test cannot provide services in the context of a TIBER test if those services create a conflict of interest. A conflict of interest exists when the professional judgement and conduct of the provider in a TIBER test is at risk of being unduly influenced by secondary interests, derived from current or previously provided services.

The CT may decide to hire a service provider that previously provided services, when both the entity and the service provider can demonstrate that the conflict of interest has ceased. The TM may object to the decision of the CT when the lack of a conflict of interest is not conclusively demonstrated. To make an informed decision, the TM may request additional documentation from the CT and the potential service provider.

In case that a service provider delivers both TI and RT services for a TIBER test, it must guarantee to have a strict separation between the delivering teams. The outcome of the Targeted Threat Intelligence report may not be unduly influenced by the RTT before the hand-over between the two teams.

3.1.8 Procurement agreements

When it comes to the procurement of service providers, the TM does not give market advice. However, the TM may give ad hoc guidance to the CT, depending on the specificities of the test. Therefore, the CTL should liaise with the TM at the very start of the preparation phase, well before making a decision on procuring which providers. When the final procurement decisions have been made, but prior to contracting, the CT must provide evidence of compliance with the requirements to the TMs. The CT must not proceed with contracting the selected providers where the TM assesses that the selected providers do not ensure compliance with the requirements in this document or where appropriate, national security legislations. The CT must keep record of the documentation provided by the TIP/RTT to evidence compliance, including detailed curriculum vitae of the staff assigned to the TIBER test.

It is not unheard of that the employees of the provider are familiar with someone working for the entity’s blue team, given the size of the cybersecurity-community. If not handled properly, this could jeopardise the confidentiality of the test. It is therefore recommended that the entity ask the provider to strictly use a code name for the entity during the internal procurement process and the quotation.

In some cases, entities may be party to an agreement with a service 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 TIP/RTT to conduct TIBER-EU tests, the prospective

TIP/RTT must meet the requirements set out in this document. In cases where such agreements are in place, the entity should liaise with the TM for further clarifications.

3.1.9 Confidentiality

The 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 providers need 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 providers should agree with the procuring entity the protocols to destroy all sensitive information[3] related to the entity and the outputs from the TIBER-EU test, once the test has been completed. Annex 4.3 and 4.5 include agreement checklists, which contain several aspects regarding confidentiality that should be included in the contract with the selected provider.

3.2 The role of the Threat Intelligence Provider

The TIP has a crucial role in the TIBER-EU process. It should provide the RTT with a Targeted Threat Intelligence Report that formulates threat scenarios aimed at mimicking potential threat actors' attacks against the live production systems that underpin the CIFs of an entity. These threat scenarios form the basis of the attack scenarios the RTT will deliver.

Creating accurate and realistic threat intelligence is a complex activity. This means that the TIP must have adequate knowledge of the threat actors, their motives, their skills and TTPs, as well an understanding of how the core elements of the financial system interact and operate. In addition, the TIP must have a good insight into the targeted entity. It needs to know for example: what the target's CIFs 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.

This will provide the RTT with the information needed to simulate a real-life and realistic attack on the entity's live systems underpinning its CIFs.

Collecting and analysing all this information and converting it into threat intelligence require specialised skills and expertise. The TIP must also have robust risk management and security controls in place, as such threat information about an

[3] 'Sensitive information' means information that can readily be leveraged to carry out attacks against the ICT systems of the financial entity, intellectual property, confidential business data and/or personal data that can directly or indirectly harm the company and its ecosystem would it fall in the hands of malicious actors.

entity is highly sensitive and may pose a threat to the entity, if the information falls into the wrong hands.

3.3 Considerations for procuring the Threat Intelligence Provider

Successful TIBER-EU tests are underpinned by a collaborative, transparent and flexible working approach observed by all TIBER-EU stakeholders. TIPs must demonstrate an ability and willingness to work in this way. This entails requirements regarding the roles present in the TIP's organisational set-up. The TIP, 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 TIPs and understand their history, organisational set-up, range of expertise and body of previous work, particularly within the financial services industry. Writing a TTIR requires an unbiased and independent view of the institution and its threat profile. Therefore, the independence of the TIP has to be ensured. A TIP that has engaged with the institution for other services (e.g. consultancy) that might introduce a conflict of interest should not be considered. If there is a conflict of interest, the CTL may not procure this service provider.

TIPs should be committed to ensuring that they act in a professional and ethical manner. Among other elements, the TIP:

- should adhere to a professional Code of Conduct. E.g. the Code of Conduct for Ethical Security Testers or the OSIRA Code of Conduct[4]; and
- should have a mature understanding of ethical standards in gathering and processing human and technical intelligence.
- Should conduct background checks on its provided experts, in accordance with national law.

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

[4] Open Source Intelligence and Research Association.

3.3.1 TI Methodology

TIPs should have robust methodologies in place to develop their threat intelligence and reconnaissance. The TIP 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 TIP:

- 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, in particular using own (private or commercially available) threat intelligence repositories, at minimum containing up-to-date threat actor profiles and their TTPs;
- conducts risk assessments and analysis; and
- can operationalise its methodologies in a clear, transparent and flexible manner.

The TIP 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 TIP 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 TIP. 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.

3.3.2 TI Staff competence

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

- staff employed by the TIP should be of irreproachable behaviour, as demonstrated by screening of criminal antecedents;
- staff employed by the TIP should be from a range of backgrounds and possess sufficient experience, e.g. backgrounds in governmental intelligence, law enforcement and financial services;

- at least one staff member employed by the TIP should have an intermediate understanding of the business model of the tested financial entity, its processes, underlying systems, sectoral challenges and threat landscape;
- the TIP 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 TIP should promote and have mechanisms to ensure continuous professional development and an R&D culture.

The TIP should have staff members that are appropriately qualified and certified for threat intelligence and open-source intelligence. More generic security certifications as well as RT certifications may be of relevance as well. However, the entity should not rely on qualifications and certifications alone; rather, the entity should actively engage with the TIP during the procurement process to gain an insight into the actual knowledge and experience of its staff.

3.3.3 Collaborative working

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

3.4 The role of the Red Team Testers

The RTT plan and execute 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 (RTTR) drafted by the RTT, which in turn feeds into the final Test Summary Report (TSR).

The RTT should expand on and execute the established threat scenarios identified by the TIP and approved by the entity. The threat scenarios are developed from an attacker’s point of view. The RTT 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 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 RTT should aim to assess the cyber resilience posture of the entity in the light of the threat it faces.

The RTT 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 RTT and the entity.

The RTT must demonstrate a willingness to work closely with the TIP, 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 RTT is expected to liaise and work with the TIP throughout the testing in order to update the threat intelligence assessment and attack scenarios with relevant and up-to-date intelligence.

3.5 Considerations for procuring Red Team Testers

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 RTT with the requisite skills are hired to perform intelligence-led red team tests, and these should not be confused with penetration testing services. Also, a provider of RTT should ensure that its testers are of the highest reputability, by conducting background checks before employment, in accordance with national laws.

The Red Team (consisting of at least three individuals) needs to fulfil the set requirements. In certain situations, the RTT may want to involve additional resources, not directly involved in the test, such as a system specialist or a technical coder. These additional resources, not part of the RT, only need to fulfil the background check requirement, and may be involved in the test after prior consultation with the TM and the CTL. It is the responsibility of the entity to ensure that the RTT meet the requirements prior to formalising any test, and therefore it should undertake thorough, documented due diligence during its procurement process. The entity should provide assurance to the TM that the RTT are compliant with the requirements in this document. Only when the TIP/RTT meet the applicable requirements, can a TIBER test be performed, as defined in the attestation.

3.5.1 RT Methodology

RTT should have robust methodologies in place to conduct the most advanced and innovative forms of red team testing. The RTT 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 RTT 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.

3.5.2 RT staff competence

RTT 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. They should also understand the business model of the financial entity, its processes, underlying systems, sectoral challenges and threat landscape. Given the unique nature of entities in the financial sector, the RTT should possess the requisite experience and knowledge of conducting red team tests on such entities.

The RTT should have 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 RTT to conduct red team tests of the highest standard, using several methodologies and different TTPs. In any case, the RTT should possess certifications that rigorously test their proficiency in RT techniques related to open source intelligence gathering, exploit development, custom malware development, Active Directory based exploitation, physical security, Human Interface Device based attack, AV/EDR/NDR/XDR, e-mail security solutions, secure web Gateway, anti-phishing solutions bypass strategies.

Additionally, they should demonstrate expertise in penetration testing across diverse environments (Web/API/Mobile Application, Mainframe, Wi-Fi), incident response skills, 'offsec' tool development, social engineering techniques and the ability to document findings clearly and communicate effectively to both technical and non-technical stakeholders. A commitment to continuous learning and adaption to the latest security threats, vulnerabilities and defence strategies is also essential.

The RTT should be able to demonstrate that its staff possess a blend of different skill sets and specialisms. Currently, the availability of RT certifications varies, with different options emerging and phasing out in various markets. Therefore, this guide does not provide a list of recommended certifications, but provides guidance on how to review the different certifications. When validating the relevant certifications, the CTL should check the following elements:

- the resources needed to achieve the certification. Is any prior education/experience needed to gain access to the certification?
- The certification provider should be well-established and have a good reputation.
- Some certifications can be obtained by answering only multiple-choice questions, whereas others require you to perform the technical tasks in a lab environment.

- Some certifications are valid for life, whereas others require you to retake an exam or collect CPE[5] credits. Also, an older certification might not have the same requirements as the same certification achieved today.
- Is the exam of the certification proctored? If not, it's possible to receive help from a colleague when achieving the exam. In some cases, the questions and answers of an exam can easily be found online.

Given the above aspects, the entity should not rely on qualifications and certifications alone. Rather, the entity should actively engage with the RTT during the procurement process, to gain insight into the actual knowledge and experience of its staff.

3.5.3 R&D capability

Good indicators of RTT technological competence are the quality and depth of their technical R&D capability. Some RTT will constantly develop specific methodologies to address different environments, such as infrastructure, security solutions (AV, XDR, NDR, EDR, Email security solutions, Secure web Gateway etc.), mainframe, web applications, wireless, mobile, etc.

3.5.4 Collaborative working

The end-to-end TIBER-EU test requires a collaborative, transparent and flexible working approach, observed by both the TIP and RTT. The RTT must demonstrate a willingness to work in this way. This might include reviewing and commenting on the TIP's deliverables, or working with the TIP to transform threat scenarios into a cohesive and tractable Red Team Test plan (RTTP). 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 RTT how they can demonstrate experience of working in a collaborative spirit with TIPs – whether within their own organisation or with another, external TIP.

[5] Continuing professional education (CPE) credits are points professionals receive for example when participating in specialized training.

4 Annex

4.1 Annex 1 - Characteristics of TI collection

Table 3

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 TIP 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 TIP 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	TIPs 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 TIP 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 TIP. For local TIBER-EU implementations, the TIP 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, TIPs 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 TIP that offers no coverage of major global languages will miss a significant proportion of relevant information. Therefore, TIPs with staff who can demonstrate fluency in key languages will offer a considerable advantage. This includes ensuring that the TIP’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 TIP 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 TIP’s retention period for such information, to gauge how long the TIP 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 TIPs which employ a variety of intelligence-gathering disciplines. TIPs 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. TIPs 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 TIP’s intelligence-gathering process life cycle must include review, operations management and quality management. The TIP 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 TIP 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 TIP 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 TIP 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 RTT 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 RTT 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).

4.2 Annex 2 - List of questions to facilitate the TI provider procurement

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 is responsible for validating the core requirements of the providers, as set out in this document, 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 this guidance.

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 in carrying out due diligence.

Reputation, history and ethics

Can the TIP 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 TIP provide at least three reference from previous assignments delivering threat intelligence for red team tests?

Has the TIP delivered services to the institution before? If yes, what were these services, and in what way do they overlap with services provided in the TIBER context? Because of these services, is there a risk that the provider is unduly influenced by secondary interests?

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

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

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

Is the TIP sufficiently insured to conduct TIBER-EU tests? More specifically, does the TIP 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 TIP's recruitment policy and process?

Does the TIP ensure that its staff members are adequately vetted?

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

Governance, security and risk management

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

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

Can the TIP 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 TIP 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 TIP ensure that no data leakage occurs from its staff's devices and teams?

Methodology

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

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

Does the TIP have access to threat intelligence from a broad range of sources, including threat actor profiles and relevant TTPs?

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

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

What mechanisms does the TIP 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 TIP take into account public data about previous incidents that would be relevant to the threats today?

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

Does the TIP 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 TIP ask for previous risk assessments or risk models exercises?

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

Does the TIP have Threat Intelligence Managers with at least five years of experience in threat intelligence?

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

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

Can the TIP 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 TIP 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 two references of previous assignments in delivering threat intelligence for red team testing activities, where at least one should be as a TI manager or deputy TI manager?

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

What qualifications do the TIP’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 the staff experienced enough in the specific dynamics of the financial services industry?

4.3 Annex 3 - Example of TI provider agreement checklist

When formalising the arrangements for a TIBER-EU test, the entity and TIP could agree on the following clauses as part of their agreement.

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 TIP 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 TIP cannot share this information with any other party without the prior approval of the entity.	
Information security	
The TIP demonstrates its security measures and procedures and how these operate. For example: the TIP has a security policy, approved by its Board of Directors; the TIP has a demonstrable effective Information Security Management System; information security is an integral part of the TIP'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 procedural and technical measures, and all access to this information is logged and monitored.	
Acceptance of provided services	
The entity and the TIP 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 TIP is transparent in the pricing of its services, including any additional or value added services.	
Continuity	
The TIP has implemented policies and procedures to ensure continuity of its services during the term of the contract.	
Audit	
The TIP 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 TIP 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 TIP 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 TIP processes personally identifiable information, it will do so according to the GDPR.	
Service quality	
The TIP 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 TIP 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 TIP 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 TIP is willing to provide the entity with the details of this process.

Responsible disclosure procedure (RDP)

The TIP and entity should agree that:

if the TIP finds vulnerabilities or other weaknesses during the research on an entity, it will disclose these to the Control Team of that entity; and

if the TIP 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 TIP 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 TIP 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 TIP provides its services to the entity.

Exit clause (general)

The TIP provides formal procedures to assure the destruction of any threat intelligence regarding the entity after the end of the contract and relationship between the TIP and the entity.

Exit clause (confidentiality)

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

4.4 Annex 4 - List of questions to facilitate the RTT procurement

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 is responsible for validating the core requirements of the providers, as set out in this document, 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 this guidance.

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 in carrying out due diligence.

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?

Has the RT provider delivered services to the institution before? If yes, what were these services, and in what way do they overlap with services provided in the TIBER context? Because of these services, is there a risk that the provider is unduly influenced by secondary interests?

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, Def Con 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) targets?

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 capable of emulating multiple advanced threat actors in a minimum of three sequential and/or parallel attack scenarios?

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 penetration testing and red team testing?

Do the Red Team members each have at least two years of experience in penetration testing and 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 of previous assignments in threat intelligence led red team tests, where at least one should be as a test manager or deputy test manager?

Can the RT 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?

Does the RT provider have a tailored technique to avoid the detection of defensive products like EDR, AV, NDR, XDR, Email security solutions, Secure web Gateway, Anti phishing solutions etc. ?

4.5 Annex 5 – Example of RTT agreement checklist

When formalising the arrangements for a TIBER-EU test, the entity and RTT could agree on the following clauses as part of their agreement.

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 Control 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 specific terminology please refer to the ECB glossary (available in English only).

PDF ISBN 987-xx-xxx-xxxx-x, ISSN xxxx-xxxx, doi:xx.xxxx/xxxxxx, QB-xx-xx-xxx-EN-N
HTML ISBN 987-xx-xxx-xxxx-x, ISSN xxxx-xxxx, doi:xx.xxxx/xxxxxx, QB-xx-xx-xxx-EN-Q