**NATIONAL BANK OF ROMANIA**

# REGULATION

No. 6 of 12.04.2022

on the framework for conducting TIBER-RO cyber resilience tests

**- 2022 -**

In accordance with Art. 2 para. (2) letter b) and with Art. 22 para. (1) and (2) of Law No. 312/2004 on the Statute of the National Bank of Romania, with Art. 404, 407 and with Art. 408 para. (1) of the Government Emergency Ordinance No. 99/2006 on credit institutions and capital adequacy, approved with amendments and supplements by Law No. 227/2007, as subsequently amended and supplemented,

Considering the TIBER-EU methodology developed at the European Central Bank's level, which establishes the European framework for testing the cyber resilience of financial institutions, by conducting controlled tests that simulate cyber attacks of advanced and persistent threats, based on information regarding cyber threats specific to the tested entity,

Pursuant to Art. 48 para. (2) of Law No. 312/2004 on the Statute of the National Bank of Romania, to Art. 405 letter c) and letter e) and to Art. 420 para. (1) of the Government Emergency Ordinance No. 99/2006 on credit institutions and capital adequacy, approved with amendments and supplements by Law No. 227/2007, as subsequently amended and supplemented,

The National Bank of Romania issues the following Regulation:

## CHAPTER I – Subject matter, scope and definitions

**Art. 1** – (1) This Regulation establishes the cyber resilience testing framework, by conducting highly complex simulated intelligence-led cyber attacks on tested entities, hereinafter referred to as the TIBER-RO Framework.

(2) This Regulation applies to financial market infrastructure administrators in the oversight area of the National Bank of Romania, hereinafter referred to as the NBR, as well as to credit institutions designated as critical participants in financial market infrastructures.

(3) Institutions participating in financial market infrastructures that are not designated as critical participants may voluntarily perform the TIBER-RO test.

**Art. 2** – For the purposes of this Regulation, the following terms and expressions have the following meaning:

(a) Information assets – data or other knowledge of value to the institution, including information and communication technology systems, their configurations, other infrastructures, as well as connections to other external and internal systems;

(b) Nation state threat actor – cyber fighting unit or group supported by a state, which cyber threatens a tested entity;

(c) Cyber threat – a potential attack, carried out primarily through information systems, by technologically advanced and persistent attackers, including organized crime groups or nation state threat actors, that affects the confidentiality, integrity or availability of resources that support critical functions of the tested entity;

(d) Active information gathering – a technique for obtaining information about the information assets of the tested entities, by engaging in direct interaction with the information systems and personnel of the tested entities and by assessing their response to various stimuli;

(e) Passive information gathering – a technique for obtaining information about the information assets of the tested entities without directly interacting with them;

(f) CTI (Cyber Threat Intelligence) – the process through which data and information are collected, analyzed and interpreted in order to identify cyber attacks and their perpetrators, and to determine key elements related to their mode of operation, motives, intentions, resources and capabilities;

(g) Blue Team – BT – all staff of the tested entity that supports performing its critical functions, with the exception of the White Team staff, whose prevention, detection and response capabilities are tested, without prior notice regarding the conduct of the test;

(h) White Team – WT – the team designated by the tested entity for the elaboration of the Scope of the test document, for the procurement of Threat Intelligence and Red Team providers and the coordination of the test, being the only structure within the entity that knows all the details related to the test and will represent the entity in relation with the NBR, the Threat Intelligence provider and the Red Team provider;

(i) Red Team – RT – the external team, which is part of the Red Team provider, that performs the simulated attack on the tested entity, in order to test its cyber resilience;

(j) TI Team (Threat Intelligence Team) – the Threat Intelligence provider's team that, based on the Cyber Threat Intelligence analysis and the Targeted cyber threat intelligence analysis, prepares the Threat Intelligence Report for the tested entity;

(k) Tested entity or institution – has the meaning provided for in Art.1 para. (2) or, as the case may be, in para. (3) of this Regulation;

(l) Critical functions – the functions of the tested entity which are necessary for the functioning of a financial market infrastructure or for its participation in financial market infrastructures, which require certain personnel, information, process and technology resources, and which, if affected, could have a significant negative impact on: the financial

stability, security and soundness of the entity, the entity's clients or the market in which the entity operates;

(m) RT provider (Red Team provider) – legal entity contracted by the tested entity to provide cyber testing services by using a Red Team;

(n) TI provider (Threat Intelligence provider) – legal entity contracted by the tested entity to provide Cyber Threat Intelligence and Targeted Cyber Threat Intelligence information services, by using a Threat Intelligence team;

(o) Critical participant – entity defined in Art. 2 point 53 of the National Bank of Romania's Regulation No. 3/2018 on the monitoring of the financial market infrastructures and payment instruments, with subsequent amendments and supplements;

(p) Red Team Test Report – formal report provided for in Art. 28 of this Regulation;

(q) TTI Report (Targeted Threat Intelligence Report) – Report on cyber threats of the tested entity, which contains the Targeted Cyber Threat Intelligence type of analysis specific to the tested entity, in the context of Cyber Threat Intelligence information on specific national cyber threats, taking into account the activities of Advanced Persistent Threats in the banking financial sector, within a period of at least 12 months before the TIBER-RO test;

(r) Cyber resilience – the capacity of an entity to anticipate cyber threats, to withstand cyber attacks, to limit the extent of the consequences of a cyber attack and to resume the activity after such attacks;

(s) Scope of the test – formal document that includes the elements provided for in Art. 20 para. (1) of this Regulation;

(t) Targeted Cyber Threat Intelligence – information regarding cyber threats of Cyber Threat Intelligence nature, which refers to at least, but not limited to: (i) the general description of Advanced Persistent Threat attacks that can attack the tested entity; (ii) the vulnerabilities of the resources that support critical functions of the tested entity; (iii) the tactics, techniques and procedures used in Advanced Persistent Threat attacks, through which the vulnerabilities of the tested entity could be exploited.

## CHAPTER II - General provisions

### SECTION 1 – General conditions

**Art. 3** – (1) The entities provided for in Art. 1 para. (2) perform the TIBER-RO test at least every 3 years, under the conditions set out in this Regulation.

(2) In order to ensure and maintain a sound risk management framework throughout the TIBER-RO test, the entity shall establish appropriate procedures, processes and controls also regarding the operations performed by the TI provider and the RT provider, in order to identify, monitor and comprehensively manage the full range of risks associated with this test.
(3) Pursuant to para. 1, entities shall ensure compliance with the requirements of the TIBER - RO test, including by concluding contracts with the TI providers and the RT providers.

**Art. 4** – (1) TIBER-RO tests, hereinafter referred to as tests, cover:

(a) the critical functions of the tested entity;

(b) the production IT infrastructure, information, procedures, personnel and outsourced services used by the entity, that support the critical functions of the tested entity.

(2) The tests simulate, in a controlled manner, cyber attacks of technologically advanced and persistent attackers, including organized crime groups or nation state threat actors, which may affect the availability, integrity and confidentiality of the resources that support the critical functions of the tested entity, using tools, methods and techniques specific to these attackers, in order to verify and improve the cyber resilience of the tested entity.

**Art. 5** – (1) The NBR monitors the tests throughout their conduct, monitoring their compliance with the requirements of this Regulation and, in case of uncompliance, requests the interruption of the testing process or the implementation of remedial measures to ensure compliance with the provisions of this Regulation.

(2) Pursuant to para. (1), the NBR provides guidance to the WT, throughout the test, endorses all the documentation prepared by the WT, TI providers and RT providers regarding the test, as well as the document provided for in Art. 31 para. (4) of this Regulation and monitors the implementation of the measures set out in the Remediation Plans.

(3) The tested entities shall submit, to the NBR, any information requested for monitoring the conduct of TIBER-RO tests.

## SECTION 2 – Test stages

**Art. 6** – The test starts with a request submitted to the NBR by the entity to be tested, according to the Annex No. 1 to this Regulation.

**Art. 7** – The test is carried out in the following successive stages:

a) Setting the test's timeframe and establishment of the WT by the entity to be tested;

b) Determination and documentation of the Scope of the test, by the WT, and its approval by the Board of the entity to be tested;

c) Selecting the TI provider and the RT provider by the WT and contracting their services;
d) Development by the TI provider of the TTI Report of the tested entity, based on the Scope of the test, in collaboration with the WT and, if necessary with the RT provider;
e) Development by the RT provider of the Red Team Test Plan of the tested entity, based on the TTI Report, in collaboration with the WT and the TI provider;
f) Application by the RT provider of the Red Team Test Plan of the tested entity, in collaboration with the WT and, if necessary, with the TI Provider;
g) Completion of the test, which implies:
   (i) preparation by the RT provider of the Red Team Test Report;
   (ii) preparation, by the structure responsible for cyber security of the tested entity, of the Blue Team Report;
   (iii) performing the replay of the test exercise, with the participation of all stakeholders involved;
   (iv) preparation by the RT provider of a summary of the test results, submitted to the NBR;
   (v) preparation by the WT of a Remediation Plan, in collaboration with the structure responsible for cyber security of the tested entity, based on the recommendations from the Red Team Test Report, approved by the Board of the tested entity.

**Art. 8** – (1) All the documents prepared regarding the testing process, as well as the related communications must be in Romanian or in English and are confidential, with a controlled dissemination regime based on the „need to know" principle.
(2) Throughout the entire process, a code name, established by the WT, must be used in order to maintain the confidentiality of the tested entity.
(3) The Red Team Test Report and the Blue Team Report are kept by the tested entity and are consulted by the NBR representatives exclusively on site.
(4) The tested entity informs the NBR, every six months, on the fulfillment of the measures established by the Remediation Plan, but not later than 15 days from the beginning of each semester.

## SECTION 3 – Limitations of TIBER-RO tests

**Art. 9** –The contractual framework concluded by the tested entity and the TI and the RT providers must contain at least:

(a) The obligation of the TI and the RT providers to maintain confidentiality regarding all the data acquired by them in the process of performing the tests;

(b) Prohibition to:

(i) destroy the equipment of the tested entity;

(ii) uncontrollably modify data, software or system configurations of the computer systems of the tested entity**;**

(iii) jeopardize the continuity of the critical functions of the tested entity**;**

(iv) disclose, outside the framework established by this Regulation, information on the threats and vulnerabilities specific to the tested entity and/or the test results.

**Art. 10** – (1) Until the completion of the test, the information regarding the test is exclusively known only by the WT, the entity's Board, the TI provider, the RT provider and the NBR.

(2) If the NBR finds, by any means, that there is information regarding the test that came to the BT's knowledge prior to the completion of the test, the NBR will inform the entity, in writing, of the obligation to resume the test from the beginning.

(3) If the NBR finds that the test is not carried out with adequate control or that the requirements of this Regulation are not complied with, it shall immediately inform the WT and request that the necessary remedial action be taken promptly. If the non-compliance persists, the NBR shall request the entity to interrupt the test until the deficiencies found are remedied.

**Art. 11** – (1) The testing is performed only by the TI and RT providers and the TI and RT members which meet the requirements set out in Annex No. 2, pre-contracted in accordance with the test specifications.

(2) In order to ensure the objectivity of the testing process, the entity may use the same TI or RT provider for performing a maximum of two consecutive tests.

## SECTION 4 – Applicable WT requirements

**Art. 12** – (1) The WT members hold an adequate range of technical skills, knowledge, experience and a high hierarchical level and have responsibilities in at least one of the following areas:

(a) operating the critical functions of the entity;

(b) continuity of the entity's activity;

(c) managing the entity's operational and IT security risks;
(d) the process of purchasing services for the entity;
(e) the provision of legal assistance relating to service contracts and the law relating to the functioning of the entity.

(2) For the application of para. (1), depending on the structure and organization of the entity, the WT shall consist of a minimum of 3 and a maximum of 7 persons holding one of the following positions or an equivalent, or belonging to one of the following categories of staff:
(a) COO (Chief Operating Officer) – The coordinator of the function that oversees the day-to-day operations of the organization;
(b) CIO (Chief Information Officer) – The coordinator of the functions of management, implementation and use of information technologies;
(c) CTO (Chief Technology Officer) – The coordinator of the function that deals with technological developments and implementations within the organization;
(d) CISO (Chief Information Security Officer) - The coordinator of the information security function.

**Art. 13** – (1) The WT is coordinated by a manager, who reports directly to the Board of the entity, represents the entity in the relation with the NBR and with the rest of the entities participating in the test and is empowered to sign any documents and contracts on behalf of the entity for the purpose of conducting the test;
(2) The WT coordinator:
(a) must have coordination skills and experience in the operation of the entity and its infrastructure (including in the Information and Communication Technology activity related to the commercial operations conducted);
(b) must preferably have experience in working with other relevant departments of the entity (e.g. operational, legal, procurement, commercial, physical security, fraud etc.) and in leading cyber resilience testing, specifically RT testing;
(3) By exception from the provisions of para. (2) letter b), in case the WT coordinator does not have any of those skills, they must be provided by other WT members.

**Art. 14** – The WT has the following responsibilities:
(a) to implement the procedures, processes and controls set out in Art. 3 para. (2) and para. (3);

(b) to develop the Scope of the test and to conduct the contracting process for the TI provider and the RT provider, monitoring the implementation of all the necessary measures to manage the risks and maintain the confidentiality of the information;

(c) to require the TI and RT providers their criminal records or similar documents attesting to the lack of criminal record of the contracted providers, of coordinators and of the TI and RT team members, in order to ensure that the criteria of good reputation, honesty and integrity are fulfilled;

(d) to approve the TTI Report, the Red Team Test Plan, the Red Team Test Report, the BT Report;

(e) to continuously monitor the compliance of the TI team and the RT with the test documentation, collaborating permanently with the NBR and ensuring the proper conduct of the test;

(f) to draft the Remediation Plan and to submit it to the Board of the entity for approval.

## SECTION 5 - Requirements applicable to TI providers and RT providers related to the contractual framework with the tested entity

**Art. 15** – The TI provider must use well-founded methodologies for documenting and identifying threats, and be able to explain their evolution and how they lead to effective results within RT tests. The methodologies must be designed so as to demonstrate to the entity that the TI provider is able to:

(a) obtain a useful context for conducting the threat analysis;

(b) document the entity's current cyber risk situation;

(c) document and substantiate the preparation of the attack;

(d) cooperate with other parties involved in testing;

(e) have a comprehensive view regarding the financial sector in which the entity operates;

(f) perform risk assessments and analyses;

(g) operate its methodologies in a clear, transparent and flexible manner.

**Art. 16** – (1) The TI provider must prepare the TTI Report, starting from the Scope of the test, and send it to the RT provider, the WT and to the NBR for review.

(2) The TI provider must collaborate with the WT and with the RT provider throughout the test, by providing assistance to the RT provider in establishing the attack scenarios and updating the information obtained as the RT attack progresses.

(3) The TTI Report does not have to be conditioned by the RT provider's experience and by the RT's ability to implement it.

(4) The TI provider and the RT provider may be the same legal entity, but the TI team staff must be different from the RT staff.

(5) The TI provider and the RT provider, respectively the staff involved in conducting the tests, must have a good reputation, honesty and integrity.

**Art. 17** – (1) The RT provider must use well-founded risk management methodologies and to:

(a) obtain a set of relevant information to ensure the penetration of the IT systems of the tested entity, based on the information in the TTI Report and the ones obtained using the methods of collecting information used by cyber attackers;

(b) record and report to the WT all actions taken during the test;

(c) have a comprehensive view of the financial sector in which the tested entity operates;

(d) develop and implement the Red Team Test Plan based on the TTI Report and taking into account the Scope of the test;

(e) cooperate with the WT and the TI provider in the development phase of the Red Team Test Plan, throughout the testing period and in the completion phase;

(f) apply, where appropriate, other attack scenarios, identified in collaboration with the TI provider and approved by the WT;

(g) follow an ethical and rigorous testing methodology;

(h) take all necessary measures to ensure that the critical functions of the tested entity are not disrupted;

(i) inform the WT, the TI provider and the NBR, whenever required or deemed appropriate, regarding the progress of the test and the objectives to be achieved during the test;

(j) elaborate and submit the Red Team Test Report to the WT and to the TI provider for review;

(k) participate in the replay of the test exercise.

**Art. 18** – (1) The requirements of this Regulation regarding the TI providers and the RT providers shall be integrated into the contractual framework concluded by the tested entities with them.

(2) The contractual framework between the tested entities and the TI and the RT providers must include clauses regarding the confidentiality and protection of personal data and provide adequate safeguards to comply with the requirements of the relevant personal data legislation.

## CHAPTER III – Development phases of the TIBER-RO Test

### SECTION 1 – Initiation of the test

**Art. 19** – (1) After receiving the request provided for in Art. 6, the NBR requires the tested entity to establish the WT and provides the entity with relevant information regarding: the testing process, the roles and responsibilities of the parties involved, as well as any other information necessary to conduct the test, in accordance with the requirements of this Regulation.

(2) The NBR may request an adjustment of the test period to ensure the effectiveness of its monitoring.

**Art. 20** – (1) In order to perform the test, the WT shall document the Scope of the test, identifying at least the following:

(a) the critical functions of the tested entity;

(b) all personnel, information, technology resources and procedures that contribute to the provision of critical functions of the tested entity, including those systems/processes/services outsourced to third parties;

(c) the targets and objectives that the RT must achieve during the test.

(2) The objectives of the test must be formulated in such manner as to demonstrate that the integrity, confidentiality or availability of resources that support the critical functions of the tested entity may be affected by an attacker, without affecting the proper functioning of the entity.

(3) The document covering the Scope of the test is approved by the Board of the tested entity.

**Art. 21** – (1) The WT procures the services of TI providers and RT providers after verifying that they comply with the requirements of this Regulation.

(2) The WT shall provide the NBR with all necessary documents and information showing that the TI and RT providers and namely the coordinators and members of the TI team and RT contracted for the test meet the minimum requirements set out in this Regulation.

### SECTION 2 - Performing the test

**Art. 22** – The TI provider performs an accurate cyber threat intelligence analysis specific to the tested entity assessed, based on the Scope of the test, the latest information on vulnerabilities and threats of a cyber nature at international level and/or on the national financial sector, as well as on the basis of professional reasoning.

**Art. 23** – (1) Following cyber threat intelligence analysis specific to the tested entity, the TI provider shall prepare the TTI Report, which the RT provider shall use in the testing phase.

(2) The analysis and elaboration of the TTI Report stage must correspond to the complexity of the tested entity, it should not last less than 5 weeks, and the collection of information must be carried out exclusively in a passive manner, in order not to alert the BT.

(3) The WT shall make summaries of test reports, prepared in previous TIBER tests, if any, available to the TI provider.

(4) The WT can assist the TI provider, at its request, with information that, in a realistic scenario, could be obtained within a reasonable period of time by an advanced and persistent attacker, in order to reduce the time required for the TI provider to formulate a comprehensive TTI Report.

**Art. 24** – (1) Based on the TTI Report, the RT provider develops the Red Team Test Plan, which details at least three cyber attack scenarios, identifying the tactics, techniques and procedures that will be used to achieve the goals and objectives set out in the Scope of the test.

(2) The WT makes summaries of test reports, prepared in the previous TIBER type tests, available to the RT provider.

(3) Cyber attack scenarios must include two attack scenarios similar to those previously suffered by financial institutions and a new scenario using elements from several real attacks.

(4) In addition to those established in para. (3), the successfully executed scenarios in the last previous TIBER type test, performed by the entity, according to this Regulation, will also be included.

(5) The test plan must also include ways of physical access within the tested entity and the possibility of the RT to introduce devices into the network of the tested entity, respectively any device that, after connecting with the technical infrastructure of the tested entity, favors the achievement of the RT attack targets.

**Art. 25** – (1) Testing is performed in a controlled and documented manner by the RT, in compliance with the Red Team Test Plan of the tested entity, following all the phases described in the plan and using only the personnel established in the contract.

(2) Upon the RT's request, the WT may decide to support the RT by providing information or a user account and/or equipment installed within the tested entity in order for the RT to overcome obstacles within a reasonable time, given the fact that an advanced and persistent attacker would have had sufficient time and resources to access the infrastructure of the tested entity.

**Art. 26** – The RT must perform the test in stages, for a period of at least 10 weeks from the start of the actual testing, to limit the likelihood of detection by the BT and must immediately inform the WT of the achievement of each objective, through the agreed channels of communication.

**Art. 27** – If the BT detects a simulated cyber attack during testing and intends to alert external partners, relevant authorities or other entities about this incident or inform the public, the WT must prevent the incident from escalating, maintain the confidentiality of the test from the BT, and to immediately inform the RT and the NBR.

## SECTION 3 - Test completion and test reports

**Art. 28** – Within 10 working days from the end of the test and the communication of this fact, in writing, to the NBR, by the WT, the RT provider, in collaboration with the TI provider, prepares the Red Team Test Report which includes:

(a) the summary of the test;

(b) the objectives achieved and the recommendations for urgent action to be taken by the entity to strengthen its cyber resilience;

(c) the List of all the actions performed by the RT provider in the test. For each action, the RT provider shall document at least, but not limited to:

(i) attack tactics, techniques and procedures used;

(ii) vulnerabilities targeted or exploited;

(iii) the necessary conditions for the attacker to fulfill the objective of the attack;

(iv) how to initiate the action on the equipment of the tested entity;

(v) the effect of the action on the devices of the computer system of the tested entity;

(vi) all changes made to the devices from the computer system of the tested entity during the action;

(vii) how the action can be detected and/or any intermediate phases of the action on the devices from the computer system of the tested entity;

(viii) how the action and/or any intermediate phases of the action on the devices of the computer system of the tested entity can be prevented;

(ix) the adequate response of the BT in case the action and/or possible intermediate phases of the action take place on the devices from the computer system of the tested entity;

**Art. 29** – (1) The BT is informed by the WT about the test and, based on the Red Team Test Report, prepares the Blue Team Report, which documents all actions taken by the BT, which

are closely related to the attack actions taken by the RT and described in the Red Team Test Report.

(2) The Blue Team Report is prepared in collaboration with the RT and approved by the WT.

**Art. 30** – After the completion of the reports provided for in Art. 28 and Art. 29, a team is created, which includes representatives of the BT and representatives of the RT, who will participate in the replay of the test and will collaborate to identify:

a) whether all RT's actions generated logs in the system journal or other relevant information in the information system of the tested entity, to indicate a possible ongoing attack so that the BT would initiate incident response procedures;
b) whether all RT's actions have generated alerts in the detection and prevention systems implemented in the tested entity's information system, so that the BT may be informed of a possible ongoing attack and initiate the incident response procedures;
c) whether the BT's incident response measures have been effective and efficient;
d) if the RT had acted differently, how appropriate the measures taken by the BT would have been;
e) ways to improve the BT's detection and response methods.

**Art. 31** – (1) Based on the recommendations from the Red Team Test Report, the WT will draft a Remediation Plan within 30 days of the completion of the test, which will be submitted for the NBR's point of view within 10 days of completion.

(2) Following the consultation of the NBR, the Remediation Plan will be submitted to the tested entity's Board for approval, which will address any deficiencies identified during testing and will set the deadlines for implementing the remedial measures.

(3) The entity has the obligation to implement the measures from the Remediation Plan within the set deadlines.

(4) The management of the tested entity will provide a certificate confirming that the test was conducted in accordance with the requirements of this Regulation, which will be submitted to the NBR for approval and will include information on the TI provider and the RT provider.

(5) The entity informs the NBR regarding the stage of implementation of the Remediation Plan, according to the provisions of Art. 8 para. (4).

## CHAPTER IV - Measures and sanctions

**Art. 32** – In case the NBR finds that the requirements of this Regulation are not complied with, it may mandate remedial measures and implementation deadlines for the entities

provided for in Art.1 para. (2), pursuant to Art. 407 of the Government Emergency Ordinance No. 99/2006, approved with amendments and supplements by Law No. 227/2007, with subsequent amendments and supplements.

**Art. 33** – If the NBR finds that the measures mandated by the NBR are not complied with and/or the remedial measures from the Remediation Plan are not properly implemented, within the established implementation deadlines, the NBR may apply sanctions to the entities mentioned in Art. 1 para. (2), in accordance with Art. 408 of the Government Emergency Ordinance No. 99/2006, approved with amendments and supplements by Law No. 227/2007, with subsequent amendments and supplements.

**Art. 34** – The provisions of Art. 32 and Art. 33 do not apply to the institutions mentioned in Art.1 para. (3).

## CHAPTER V - Final provisions

**Art. 35** – TIBER-RO tests may be initiated after 30 days of the date this Regulation takes effect, but not later than 3 years from the date this Regulation takes effect.

**Art. 36** – Annexes No. 1 and 2 are an integral part of this Regulation.

**Art. 37** – This Regulation is published in the Romanian Official Journal, Part I and takes effect on the date of publication.

Chairman
of the National Bank of Romania's Board

MUGUR ISĂRESCU

Annex No. 1

Request for TIBER-RO test

| | |
|---|---|
| Date of the request | |
| Name | |
| Social headquarters | |
| Name and contact information | |
| Proposed testing period | |

Annex No. 2

Requirements, certifications and qualifications applicable to TI and RT providers

I. Requirements applicable to TI providers

A) The TI provider (legal entity) must:

1) present at least 3 references from financial institutions, national or from abroad, for which it provided Threat Intelligence Reports;

2) have a civil liability insurance in force, applicable for the activities that have been agreed on in the contract and/or that result from incorrect conduct, negligence etc.

B) The Threat Intelligence Manager must:

1) have at least 5 years of experience in threat intelligence reporting, including three years of producing threat intelligence for the financial services industry;

2) provide an updated Curriculum Vitae, showing experience in the field and at least 3 references from financial institutions regarding threat intelligence reports ;

3) preferably be certified in at least one of the qualifications mentioned in point III;

4) if point 3) is not fulfilled, the TI team manager must be certified in at least one of the qualifications mentioned in section IV.

C) The members of the TI Team must:

1) have at least 2 years of experience in threat intelligence reporting;

2) provide an updated Curriculum Vitae, which showcases the experience in the field;

3) be certified in at least one of the qualifications mentioned in point IV;

4) the TI Team must have a multidisciplinary composition, with a broad range of skills (eg OSINT – Open-source intelligence, HUMINT – human intelligence and geo-political knowledge).

## II. Requirements applicable to RT providers

A) The RT provider (legal entity) must:

1) provide at least 5 references from financial institutions, national or from abroad, regarding penetration tests performed, preferably intelligence-led Red Team tests;

2) have a civil liability insurance in force, applicable for the activities that have been agreed on in the contract and/or that result from incorrect conduct, negligence etc.

B) The RT manager must:

1) have at least 5 years of experience in Red Team testing, including at least 3 years in the financial services industry;

2) provide an updated Curriculum Vitae, showing experience in the field and at least 3 references from financial institutions regarding Red Team penetration tests performed;

3) be certified in at least one of the qualifications mentioned in point III;

C) The RT members must:

1) have at least 2 years of experience in Red Team testing of the IT infrastructure, in the financial services industry;

2) provide an updated Curriculum Vitae, which showcases the experience in the field;

3) be certified in at least one of the qualifications mentioned in point IV;

4) the RT must have a multidisciplinary composition, targeting a broad range of skills (such as business knowledge, penetration testing, reconnaissance, threat intelligence, risk management, social engineering, vulnerability analysis or combinations thereof).

III. Certifications of TI Team Managers or RT Managers:

| Certification institution | 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)* |

IV. Certifications of TI Team members or RT members:

| Certification institution | 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 | *eLearnSecurity 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)* |
| Other | *EC-Council Certified Security Analyst (ECSA)* |
| | *Licensed Penetration Tester (LPT)* |
| | *Certified Ethical Hacker (CEH)* |