TIBER-PT
RISK MANAGEMENT

TIBER-PT
RISK MANAGEMENT

MARÇO 2022

BANCO DE PORTUGAL
EUROSISTEMA

Lisboa, 2022 • www.bportugal.pt

Table of Contents

Change Log

Version	Date	Comments

1 Disclaimer

[Target Entity], as a participant in a TIBER-PT test, is entirely responsible and liable for conducting proper and timely risk management based on best practices, in accordance with the TIBER-PT implementation guide. The Banco de Portugal (BdP) and the TIBER-PT Cyber Team (TCT) may under no circumstances be held accountable for the risk management of a TIBER-PT test.

2 Introduction

2.1 Purpose of this document

Taking into consideration the critical nature of the functions targeted by a TIBER-PT test, it is paramount that the target entity effectively identify the risks associated with the test beforehand and implement the necessary risk controls and mitigating actions in a timely manner, to ensure that the test is conducted in accordance with the entity's own risk appetite and according to best practices in risk management.

The entity must understand the likelihood of the test causing a denial-of-service incident, an unexpected system crash, damage to critical live production systems, or the loss, modification or disclosure of data for the employment of a robust risk management throughout the preparation, execution and closure of the TIBER-PT test. It is expected that as the test progresses the entity continuously (re-)assesses the risks that may arise and takes the necessary actions,

Section 4 of this template corresponds to a non-exhaustive list of risk categories where risk management may be required. Yet, given its non-exhaustive nature, the entities may adjust the structure of the risk identification table, to ensure completion, as long as these risk categories are still addressed.

This template is filled out by [Target Entity] to document the risks associated with the TIBER-PT test and identified by [Target Entity] as well as the controls, processes and procedures implemented to guarantee that the test is carried out in a controlled manner and risks have been adequately managed. This document shall be shared with the TCT, in a timely manner, before the beginning of the testing phase. Any other relevant documents that describe these risks and mitigating actions shall also be made available to the TCT, and may be referenced in the Risk Identification document. Any further changes to this document must also be shared in a timely manner with the TCT.

2.2 Structure of this document

Section 3 of this document contains a table (Table 3.1 •) in which the entity shall identify the risks associated with the TIBER-PT test. This table is composed of four columns: the risk ID number; the risk category; the risk description and the risk score (resulting from the likelihood of materialization and impact). This table is complemented by Table 3.2 • , which shall detail the mitigation actions, meaning the controls, processes and procedures established to contain and mitigate the risks, for each possibly impacted asset. These tables shall be extended with extra rows as required.

Section 4 of this document contains a short description of each of the risk categories that could be considered by the entity, and a non-exhaustive list of considerations that the entity shall take into account when managing the risks associated with the tests.

3 Risk Identification table

A risk assessment should be conducted prior to a TIBER-PT test to ensure proper risk management is in place and in line with the target entity's existing risk management framework. This assessment should build upon information from different sources, namely, but not exclusively: i) business and system overview documentation (for systems included in the test scenarios); ii) business impact assessments and; iii) lists of system owners/contacts/availability.

Table 3.1 • Risk Identification table

Risk ID	Type	Risk	Risk Score (Likelihood x Impact)
1.1	Legal and provider risks	[Target Entity to insert text]	[Target Entity to insert text]
1.#	Legal and provider risks	[Target Entity to insert text]	[Target Entity to insert text]
2.1	Reputational and ethical risks	[Target Entity to insert text]	[Target Entity to insert text]
2.#	Reputational and ethical risks	[Target Entity to insert text]	[Target Entity to insert text]
3.1	Crisis and incident escalation risks	[Target Entity to insert text]	[Target Entity to insert text]
3.#	Crisis and incident escalation risks	[Target Entity to insert text]	[Target Entity to insert text]
4.1	Operational red teaming risks	[Target Entity to insert text]	[Target Entity to insert text]
4.#	Operational red teaming risks	[Target Entity to insert text]	[Target Entity to insert text]

5.1	Operational blue teaming risks	[Target Entity to insert text]	[Target Entity to insert text]
5.#	Operational blue teaming risks	[Target Entity to insert text]	[Target Entity to insert text]
6.1	Clean-up risks	[Target Entity to insert text]	[Target Entity to insert text]
6.#	Clean-up risks	[Target Entity to insert text]	[Target Entity to insert text]
7.1	Project risks	[Target Entity to insert text]	[Target Entity to insert text]
7.#	Project risks	[Target Entity to insert text]	[Target Entity to insert text]
8.1	Other	[Target Entity to insert text]	[Target Entity to insert text]
8.#	Other	[Target Entity to insert text]	[Target Entity to insert text]

Table 3.2 • Risk mitigation table

Risk ID	Asset	Threat	Mitigating Actions	Comment
1.1	[Target Entity to insert text]	[Target Entity to insert text]	[Target Entity to insert text]	[Target Entity to insert text]
1.#	[Target Entity to insert text]	[Target Entity to insert text]	[Target Entity to insert text]	[Target Entity to insert text]
2.1	[Target Entity to insert text]	[Target Entity to insert text]	[Target Entity to insert text]	[Target Entity to insert text]
2.#	[Target Entity to insert text]	[Target Entity to insert text]	[Target Entity to insert text]	[Target Entity to insert text]
3.1	[Target Entity to insert text]	[Target Entity to insert text]	[Target Entity to insert text]	[Target Entity to insert text]
3.#	[Target Entity to insert text]	[Target Entity to insert text]	[Target Entity to insert text]	[Target Entity to insert text]
4.1	[Target Entity to insert text]	[Target Entity to insert text]	[Target Entity to insert text]	[Target Entity to insert text]
4.#	[Target Entity to insert text]	[Target Entity to insert text]	[Target Entity to insert text]	[Target Entity to insert text]

5.1	[Target Entity to insert text]	[Target Entity to insert text]	[Target Entity to insert text]	[Target Entity to insert text]
5.#	[Target Entity to insert text]	[Target Entity to insert text]	[Target Entity to insert text]	[Target Entity to insert text]
6.1	[Target Entity to insert text]	[Target Entity to insert text]	[Target Entity to insert text]	[Target Entity to insert text]
6.#	[Target Entity to insert text]	[Target Entity to insert text]	[Target Entity to insert text]	[Target Entity to insert text]
7.1	[Target Entity to insert text]	[Target Entity to insert text]	[Target Entity to insert text]	[Target Entity to insert text]
7.#	[Target Entity to insert text]	[Target Entity to insert text]	[Target Entity to insert text]	[Target Entity to insert text]
8.1	[Target Entity to insert text]	[Target Entity to insert text]	[Target Entity to insert text]	[Target Entity to insert text]
8.#	[Target Entity to insert text]	[Target Entity to insert text]	[Target Entity to insert text]	[Target Entity to insert text]

4 Risk Categories

4.1 Legal and provider risks

During a TIBER-PT test, the Threat Intelligence Provider (TIP) and Red Team (RT) provider will get significant knowledge about exploitable vulnerabilities and security breaches in the infrastructure and systems of the target entity. The target entity must have a clear understanding of these confidentiality and provider risks and address it through Risk Management controls, processes and procedures. This can be achieved, for instance, through the contractual agreements made between the target entity and the TIP and RT provider.

Moreover, the target entity must consider the legal risks associated with the contractual arrangements, namely those related with liability, insurance and consent.

Considerations to take into account when managing legal and provider risks (non-exhaustive list)

- Confidentiality
  - RT gets access to highly confidential material, for instance, financial statements/insider information/legal issues, etc.;
  - Possibility of early disclosure of the test due to lack of experience or skills within the RT provider;
  - Staff changes among RT testers, especially for RT lead phases of the test (which might also affect other considerations besides confidentiality);
  - Usage of non-disclosure agreements (NDA).
- Compliance
  - Regulatory (ensure compliance with regulatory requirements within all areas of the business)
  - Rules of engagement (ensure RT's internal procedures are compliant with the rules of engagement)
- Procedures
  - The entity and the TIP and RT provider must formally agree on at least the following aspects: the scope of the test, boundaries, timing and availability of the providers, contracts, actions to be taken and liability.
  - Definition of how and where the test infrastructure will be set-up, namely the location where the attack infrastructure will be hosted (i.e. Command & Control servers), the access to the target entity's infrastructure from test participants and how the information the RT will be collecting (retrieved information, logs, test results/evidence, confidential information at rest or in transit) shall be collected, processed and stored.

4.2 Reputational and ethical risks

The occurrence of undesirable consequences with external visibility from the execution of a TIBER-PT test might lead to loss of customer confidence, exposure to the media and associated risks like a fall in share prices.

These undesirable consequences might originate, for instance from a lack of effective data protection, leakage of information based on the intelligence gathering by the TIP or the possible success in "attacks" by the RT, which may compromise systems and cause outages.

Risks may also arise from the lack of clear ethical rules for the execution of the test, which should set the limits, for instance, which methods the TIP can use to gather intelligence and how the RT provider can conduct their attacks.

Considerations to take into account when managing reputational and ethical risks (non-exhaustive list)

- Ensure that the RT adheres to all international and national laws and regulations;
- Must follow highest standard of ethical conduct;
- Ensure that tests will only be performed within the scope of the engagement, that any infraction will always be reported to the White Team Lead (WTL) and that there mitigation controls are in place;
- Information or privileges gained can only be used in the context of the test and in accordance with the rules of engagement.

4.3 Crisis and incident escalation risks

During a TIBER-PT test, it is expected that the target entity will need to trigger incident escalation. The target entity shall therefore ensure that adequate controls are in place so that the WT can control any escalations related to the TIBER-PT test, both in the sense of the incident management itself, as well as avoiding undesirable disclosures of the test to avoid invalidating the remainder of the test.

Considerations to take into account when managing crisis and incident escalation risks (non-exhaustive list)

- Control critical incidents that might arise as a result of testing through the definition of procedures for managing incidents during the TIBER-PT test, namely:
    - Define procedures to clarify if an incident is related to the test;
    - Understand trigger actions and ensure that the internal escalations line can be "intercepted" and controlled;
    - Define internal communication lines with areas involved in Incident Management functions and Incident Escalation Lines;
    - Plan for this kind of activity (including in case of false positive incidents) – resource and time management.
- Knowledge of clearly defined technical and business procedures for handling security incidents:
    - General procedures;

    - System specific procedures.
- Develop use cases to understand how the WT can manage incidents that could happen during the test phase. These use cases shall define where in the escalation lines the information lines shall be stopped and how to respond to avoid disclosure of the test. Moreover, these use cases shall specify what types of incidents may halt the test and which ones shall not have an impact in the continuation of the test.

4.4 Operational red teaming risks

At all times during a test, the WT must be in control of the RT activities. This includes having a clear set of communication guidelines and a mutual understanding of the WT's risk appetite and the boundaries set for the test activities. Due to the intrusive nature of the test activities, insufficient control by the WT may cause significant impacts to the target entity like system unavailability or deletion of data. Thus, it is essential that test activity is well documented, up to date and accessible to the WT at all stages of the test.

The WT should consider all the systems in the scope of the TIBER-PT test, as well as the systems that support any critical functions, so that depending on the risk appetite of the target entity, it can effectively determine the boundaries for the RT in what regards to what specific systems can be attacked and in what manner.

Considerations to take into account when managing operational red teaming risks (non-exhaustive list)

- Define acceptance and authorisation criteria and procedures for different risk/impact levels;
- Define processes for follow-up and validation of risks/impacts (e.g. attack scenario validation and status meetings);
- Establish an approval hierarchy (e.g. replacements in case of absence of the WTL) and procedure for the RT in case it cannot obtain a response from the WT;
- Assess the acceptable timings to conduct the tests and what periods pose too high a risk (e.g. important dates or hours during a day). Such cases may include (not exclusively): IT change freeze periods; system roll-outs; and co-existence with other test activities;
- Conduct thorough due diligence of in-scope systems prior to any testing to ensure that backup and restoration capabilities are in place;
- Assess what actions are known to make systems unstable (e.g. large amounts of data passing through an application);
- Clearly define what disruptive activities must not be performed (e.g. locking out users or deleting/moving files without backups), including criteria for user correspondence, for instance, phishing mail contents (type of language, contents to avoid and approval procedures before sending);
- Determine the escalation procedures between the RT and WTL and *vice versa*;
- Establish a "Red button" procedure to allow the WT to halt the test immediately;
- Establish secure channels of communication between WT, TIP, RT and TCT to ensure an adequate confidentiality level (e.g. physical meetings and secure mail);
- Document sufficient contact information of all participants:
    - RT and WT contacts (incl. mobile numbers of the RT and WTL);

    - Availability (planned holidays, on/off business hours, which RT testers are active and when).
- Establish a schedule of regular updates on testing activities (e.g. weekly physical meetings and daily calls) and the kind of information expected from the RT:
    - Deviations from TIP recommendations;
    - Deviations to original test scenarios;
    - Deviations to the plan;
    - RT's risk considerations for upcoming activities
    - RT log updates or other material indicating ongoing success level.
- Define and document the required clean-up activities including instructions for removal of malware – during and after the completion of the test:
    - Kill switch/Self-destruct mechanisms;
    - File less malware – reboot automatically to do clean-up;
    - Phishing mails;
    - Domain whitelisting (if something for instance was blacklisted during test);
    - Password reset.
- Protect access to Web shells (e.g. password protection)

4.5 Operational blue team risks

One of the key aspects of a TIBER-PT test (in accordance with the TIBER-EU framework itself) is that the BT especially shall not be made aware of the test before the closure phase. An alerted BT might behave differently to what would occur in case of a real threat or take further preventive measures which could lead to false test results.

Yet, considering the impact that the actions of the RT during the test might have on an unaware BT, this may require an abnormal volume of defensive activities which may overload the BT which could in-turn lead to actual real attack activities not being prioritised. It is important for the WT to address these risks, for instance by ensuring cover-up stories, by having agreed procedures for how to halt a test (either temporarily or altogether) and by generally being aware of BT activities.

Considerations to take into account when managing operational blue teaming risks (non-exhaustive list)

- Assess the WT's capacity to stop incident escalations that could happen 24/7 and ensure sufficient understanding and knowledge of BT activities;
- Define a strategy for managing BT/others:
    - Define criteria and procedures to inform the Blue Team (in a controlled manner) if they make inquiries;
    - Have cover stories prepared and agreed within the WT;
    - Ensure on a continuous basis that the BT will not become aware of the TIBER test;
    - Avoid BT overload (e.g. extended amount of hours/overtime because of the test).
- Determine the procedures in case of a real attack happens during the testing phase;
- Assess the WT and BT capacity to effectively respond to real attacks, considering the elevated risk posed during the testing phase.

4.6 Clean-up risks

This risk category encapsulates the risks arising from planned clean-up procedures which might include: Command and Control Infrastructure deactivation, removal of malware and backdoors, passwords revealed/discovered that should be changed, data collected by the TIP and RT securely managed, etc.

Management of these risks shall take into consideration the possibility that, for instance, compromised credentials belonging to accounts in which changing a password might prove difficult or have unintended consequences (e.g. system accounts), or that kills switches built into malware might fail.

Considerations to take into account when managing clean-up risks (non-exhaustive list)

- Information/data clean-up activities by the TIP and RT after the conclusion of the test (e.g. threat intelligence, findings, reports).
- Assess the existence of system accounts or similar accounts in which changing access credentials may have significant impact and determine how to proceed for each of these cases;
- Protect test documentation (e.g. Red Team test report) from unauthorised disclosure;
- Safeguard and protect data extracted during test that contains sensitive data (within the entity being tested as well as within TIP and RT);
- Establish procedures for managing future back-up restauration which may contain malware or tools installed during the test;
- Lack of clean-up activities on RT side even though stated in contract.

4.7 Project risks

Any project has intrinsic risks associated like deviations to the plan, which shall nonetheless be addressed during a TIBER-PT test.

Also, other concerns more specific to a TIBER-PT test need to be considered, namely those that may invalidate the test, like the risks of the BT acknowledging that a RT test is or will be in progress before reaching the closure phase. The WT might be required to make up cover stories to protect the integrity of the test.

Considerations to take into account when managing project risks (non-exhaustive list)

- Disclosure of test results (deliberately or inadvertently);
- Scope creep;
- Ensuring sufficient trust level of the RT test report;

- Financial risk (overspending);
- Resource management.

4.8 Other

This should be seen as a catch-all category for all risks not addressed in the prior sections.

Other considerations to take into account when managing risks (non-exhaustive list)

- A WT extension may be arranged, subject to TCT approval, to ensure that risks associated with the actual test are managed properly. Evaluation of operational risks might need to involve security experts and senior management exclusively for this purpose as part of the extended WT. Tasks for this WT extension could be:
    - To review test activities to mitigate risks prior to testing, including acceptance or decline of test scenarios, without compromising the effectiveness of the exercise;
    - To establish criteria for the assembly or consultation of the WT extension;
    - To enable a robust and smooth procurement process.
- Risks identified from findings should be managed/registered for further action/follow-up.