blog.nviso.eu /2024/08/29/the-big-tiber-encyclopedia/

The Big TIBER Encyclopedia

Jonas Bauters ⋮ 22-28 minutes ⋮ 8/29/2024

TIBER (Threat Intelligence-Based Ethical Red Teaming) is a framework introduced by the European Central Bank (ECB) in 2018 as a response to the increasing number of cyber threats faced by financial institutions. The framework provides a standardized methodology and guidelines for conducting controlled and targeted realistic cyberattack simulations. The key objective of TIBER is to assess and improve the resilience of financial institutions against cyber threats by adopting a proactive approach.

The results of the exercises provide valuable insights into areas that need improvement, enabling organizations to enhance their cyber defenses and better protect themselves against real-world cyber threats.

The European framework is known as TIBER-EU, which can be voluntarily adopted by individual countries, driven by the national competent authority (NCA) for the financial sector of that member state, which is in many cases also the central bank. In the meantime, 16 countries (as well as the ECB, adding up to 17 implementations) have adopted the framework and apply it:

As of January 17th, 2025, the DORA regulation will apply for relevant financial entities and ICT third-party service providers. Threat-led Penetration Testing (TLPT) as required by the DORA regulation will be specified in accordance with TIBER-EU and in agreement with the ECB.

The purpose of this blog post is therefore threefold. Firstly, we want to provide an overview of the current country-specific implementations of the TIBER-EU framework and where these implementations may differ (even if only slightly). Secondly, we want to add some lessons learned and personal insights gained from the execution of multiple TIBER engagements over the past few years for different TIBER jurisdictions. These are added in the blue-lined quote boxes. Thirdly, we want to show why TIBER still makes sense ahead of DORA TLPT and will continue to make sense once the regulation is applied.

To get started, which countries have their own implementation of the TIBER-EU framework and how is their implementation guidance provided? Note that we also add the TIBER-EU framework documentation as a reference, which should not be considered an implementation document.

Jurisdiction	Guidance Format	Language	Latest Version	Introduction Date	Reference
Europe 🇪🇺	PDF	EN	May 2018	May 2018	TIBER-EU
Austria 🇦🇹	PDF	EN	November 2023	November 2023	TIBER-AT

Belgium 🇧🇪	PDF	EN	December 2022	June 2020	TIBER-BE
Denmark 🇩🇰	PDF	EN	December 2021	December 2018	TIBER-DK
Finland 🇫🇮	Web Page	EN	Updated annually	April 2020	TIBER-FI
France 🇫🇷	PDF	EN	January 2024	January 2024	TIBER-FR
Germany 🇩🇪	PDF	EN	December 2022	Summer 2019	TIBER-DE
Iceland 🇮🇸	PDF	EN	June 2023	February 2023	TIBER-IS
Ireland 🇮🇪	PDF	EN	December 2019	December 2019	TIBER-IE
Italy 🇮🇹	PDF	EN	August 2022	Early 2020	TIBER-IT
Luxembourg 🇱🇺	PDF	EN	Not specified	November 2021	TIBER-LU
Netherlands 🇳🇱	PDF	EN	December 2022	2016	TIBER-NL
Norway 🇳🇴	PDF	EN	October 2022	May 2021	TIBER-NO
Portugal 🇵🇹	PDF	EN	February 2024	April 2022	TIBER-PT
Romania 🇷🇴	Web Page PDF	RO EN	May 2022	May 2022	TIBER-RO
Spain 🇪🇸	PDF	EN	January 2022	December 2020	TIBER-ES
Sweden 🇸🇪	PDF	EN	Not specified	December 2019	TIBER-SE

Availability of TIBER guidance

Note that we refer to the country-specific TIBER websites and not directly to the implementation PDFs to avoid dead links as much as possible. However, if you would notice one of the links no longer working, don’t hesitate to reach out so we can update it.

Most countries follow the same approach, i.e. an English guidance PDF. However, there are some exceptions:

- TIBER-FI uses a web page in English
- TIBER-RO uses a web page in Romanian (although a PDF extract is also available)

Finland 🇫🇮 has packed their implementation guide in a series of web pages describing participants to a TIBER exercise, providing supporting materials, and outlining procedures for the different phases.

Interestingly, Romania 🇷🇴 has a unique approach to their TIBER guidance, which looks more like a regulation having specific articles that must be implemented.

For a consistent offering, the NCA would need to provide at least a TIBER landing page with a small introduction on the website, containing a link to their guidance PDF and other documents in English.

Anyhow, let’s now deep-dive into the implementation guidance to see how each country implements TIBER-EU!

Major Implementation Aspects

Test Duration

First, we’re looking at test duration, which would be straightforward to consistently describe across jurisdictions when simply basing it on the TIBER-EU recommendations. However, as you can see from the table below, six countries have at least one phase for which no suggested duration is mentioned. Only two countries do not mention any duration at all, which also coincides with those countries who use a web page for their guidance (Finland 🇫🇮 and Romania 🇷🇴). All durations are listed in weeks:

Jurisdiction	Preparation	Threat Intelligence	Red Team	Closure
TIBER-EU 🇪🇺	4-6	5	10-12	4
TIBER-AT 🇦🇹	4-6	4-6	12-14	4-6
TIBER-BE 🇧🇪	12-14	4-6	12	6 weeks to months
TIBER-DE 🇩🇪	No mention	6	12	No mention
TIBER-DK 🇩🇰	12-16	6	12	8
TIBER-ES 🇪🇸	4-6	5	10-12	4

TIBER-FI 🇫🇮	No mention	No mention	No mention	No mention
TIBER-FR 🇫🇷	12-14	4-6	12-14	4-8
TIBER-IE 🇮🇪	4-6	5	10-12	4
TIBER-IS 🇮🇸	12-16	6	16	8
TIBER-IT 🇮🇹	4-6	5	10-12	4
TIBER-LU 🇱🇺	4-6	6-8	12	6
TIBER-NL 🇳🇱	6-8	6-8	10-12	6-12
TIBER-NO 🇳🇴	4-6	No mention	10-12	No mention
TIBER-PT 🇵🇹	4-6	5-6 (but can be extended to 8)	10-12	4
TIBER-RO 🇷🇴	No mention	No mention	No mention	No mention
TIBER-SE 🇸🇪	No mention	No mention	10-12	No mention

TIBER phase duration in weeks

Most durations are similar to the TIBER-EU estimates, but we do have a few additional interesting observations to make:

- Some jurisdictions (🇧🇪, 🇩🇰, 🇫🇷, 🇮🇸) have explicitly included procurement in the preparation phase duration (and thus increased it accordingly). For others, procurement is still part of preparation but not specifically counted in the duration.
- The TI (around 6 weeks) and RT (around 12 weeks) phases are fairly consistent but the closure phase varies more across country implementations.

However, if you have performed a TIBER exercise, you can probably attest that the suggested durations are not always how it goes in practice and planning/execution may vary.

> While the duration of the red teaming phase has been fairly consistent across exercises, we have seen variations in closure phase duration from 2 weeks to +6 months.

As such, the static number of weeks in the implementation guide should not be considered a hard requirement (at least for TIBER). TLPTs under DORA will require more discipline with regards to timelines however.

Generic Threat Landscape (GTL)

The Generic Threat Landscape or GTL is a national threat intelligence report outlining the geopolitical and criminal threats facing the financial sector for that jurisdiction. It is typically used:

- as part of the preparation phase, to guide the scoping discussions
- during the testing phases, as a basis for the targeted threat intelligence report

TIBER-EU mentions that the GTL is an optional element that can be included by the member states in their TIBER-XX implementations. Certain implementations consider it important enough to include it by default, while others repeat the optional character and thus not require it to be used:

GTL Included	GTL Optional	GTL Not Mentioned
🇦🇹 🇧🇪 🇩🇪 🇩🇰 🇫🇮 🇫🇷 🇮🇸 🇳🇱 🇳🇴 🇸🇪	🇪🇺 🇪🇸 🇮🇪 🇮🇹 🇱🇺 🇵🇹	🇷🇴

GTL Usage

Most TIBER jurisdictions require the usage of a GTL that is regularly updated. The most common GTL update frequency is on an annual basis (🇪🇺 🇩🇰 🇮🇸 🇮🇹 🇳🇱 🇳🇴 🇸🇪), with a number of TCTs (such as Belgium 🇧🇪, Ireland 🇮🇪, Austria 🇦🇹, and Germany 🇩🇪) having updates to the GTL twice per year. France 🇫🇷 keeps it more vague and talks about "regular" updates. Nearly one third of jurisdictions lists the GTL as an optional aspect, with Portugal 🇵🇹 explicitly mentioning that no GTL is/was available at the time of writing.

Purple Teaming

The TIBER-EU framework includes mention of an optional purple teaming component as part of the closure phase, "in which the blue team (BT) and the red team (RT) provider work together to see which other steps could have been taken by the RT provider and how the BT could have responded to those steps". Even though it is optional, the ECB (in collaboration with implementing countries at that time) has published a purple teaming best practices document in 2022 to provide additional guidance: TIBER-EU Purple Teaming Best Practices

This guidance document presents purple teaming as a collaborative activity that may be performed in the testing phase (as a last resort option for execution) as well as the closure phase. Let's have a look whether country-specific implementations also include purple teaming guidance:

PT Required	PT Optional	PT Not Mentioned
🇦🇹 🇩🇪 🇮🇪 🇱🇺 🇳🇱	🇪🇺 🇧🇪 🇩🇰 🇪🇸 🇫🇮 🇫🇷 🇮🇸 🇮🇹 🇳🇴 🇵🇹	🇷🇴 🇸🇪

Purple Teaming inclusion in the guidance

Five countries not only mention purple teaming, but even include it as an obligatory phase. Ten countries include it as an optional step, while the remaining two do not mention purple teaming at all. We can thus conclude in terms of purple teaming, there is a big difference between countries' guidance!

In practice, purple teaming has always been included in our exercises, either as

> part of the closure phase, during execution, or both, resulting in greatly added value. The benefit of purple teaming during the execution phase is that it allows to validate certain riskier steps towards critical economic functions (CEF) which you may otherwise not have performed.

The TIBER-BE 🇧🇪 implementation guide contains most details regarding the execution of purple teaming, including input on purple teaming as part of scenario execution during the testing phase.

We can see however that implementations updated after the release of the TIBER-EU 🇪🇺 purple teaming best practices make a reference to this document, even in case purple teaming is only an optional element. In addition, we want to point out that while purple teaming in the closure phase is optional, purple teaming during the testing phase is something situational. Therefore, countries which might not require a purple team exercise in the closure phase might refer to the document for the last resort purple team efforts during the testing phase.

Leg-up

Another important aspect to TIBER is the principle of leg-ups. In case the red team provider is unable to proceed with their attack chain (either due to preventive controls, time limitations, a lack of information, ethical considerations, or other reasons), they can be provided with some assistance from the white team (WT). This allows them to continue the test, focus on the next flag, and identify additional improvement points. In terms of leg-up input, we can make two major distinctions: either there is no mention at all, or it is briefly mentioned that the possibility of using leg-ups exists:

Leg-ups Mentioned	Leg-ups Not Mentioned
🇪🇺 🇦🇹 🇧🇪 🇩🇪 🇩🇰 🇪🇸 🇫🇮 🇫🇷 🇮🇪 🇮🇸 🇮🇹 🇱🇺 🇳🇱 🇵🇹	🇳🇴 🇷🇴 🇸🇪

Guidance on leg-ups

The fact that leg-ups are not mentioned, does not mean they are not applied in those respective countries' exercises however. This just means the implementation has no additional input on top of what is mandated by the TIBER-EU framework. In addition, the White Team is allowed to share information with the TI or red team according to their own appetite.

There is one jurisdiction that does not just mention leg-ups, but even has a dedicated section on leg-ups (and a separate leg-up document) with the different types of assistance that can be provided: Belgium 🇧🇪. The latest update of the TIBER-BE 🇧🇪 specification comes with a lot of additional useful information on leg-ups, that we would love to see propagated across countries.

> We often notice difficulties on the entity's side to prepare leg-ups in time. From the White Team's perspective; when you receive the red team test plan (RTTP), make sure to communicate to the Red Team which leg-ups are feasible and which are not. Start preparing them well in advance!

Scenario X

The main idea for TIBER scenarios is the emulation of the most relevant threat actors and their Tactics, Techniques, and Procedures (TTPs). Scenario X allows to think outside of the box and devise a scenario making use of the red team's more creative or innovative TTPs. TIBER-EU 🇪🇺 does not use the term "Scenario X", but describes the possibility for a creative scenario nonetheless. We have distinguished three options that are distributed evenly across jurisdictions:

- Scenario X is included and described in the guide.
- Scenario X is not explicitly mentioned but the guide does mention physical testing. In these cases, there is no focus on a generally creative scenario, however.
- There is no mention of scenario X nor physical testing.

Scenario X Mentioned	Physical Testing Mentioned	No Mention
🇧🇪 🇫🇷 🇮🇪 🇮🇹 🇳🇱 🇳🇴	🇪🇺 🇦🇹 🇩🇪 🇱🇺 🇵🇹 🇷🇴	🇩🇰 🇪🇸 🇫🇮 🇮🇸 🇸🇪

Scenario X or physical testing

However, even in case scenario X or a physical scenario is not explicitly mentioned in the implementation guide, the respective TCT will definitely welcome the suggestion if this would benefit the financial entity.

> Around 85% of our TIBER exercises included a physical testing component as part of a scenario X.

For clarity, a physical scenario and scenario X are not necessarily the same thing or always linked together. It is possible to have a scenario X without physical, where the red team can employ creative cyber TTPs, think out of the box, and be forward looking. It is also possible to have a physical component in a regular threat scenario, if there is threat intelligence to support it. Often though, the entity itself is interested in seeing a physical attack scenario, which fits best under scenario X if there is insufficient threat intelligence to support it.

There are many more aspects on which we could compare TIBER implementation guides, but we consider the ones above to be major differentiating points.

Minor Implementation Differences

Many other aspects are fairly consistent across the different jurisdictions. The following items are less significant items or minor differences that are worth mentioning briefly.

Risk Management

A TIBER test is not without risk since the red team will be targeting critical production systems. The TIBER-EU 🇪🇺 specification contains a detailed section on risk management, providing input on a risk assessment, provider requirements, contracting, confidentiality & escalation procedures, and risk management during the execution.

> When the White Team has a risk management document prepared, we can include these risks in the red team test plan (RTTP) and further update them throughout the exercise, providing additional assurance that risks are identified, understood, and managed where needed.

All the implementation guides make at least a mention of risk management, but some keep the information to a bare minimum.

Cross-jurisdictional Testing

It is of course possible that the entity being subjected to TIBER testing has a presence in different countries and would thus fall under different/multiple jurisdictions. In this case, the TIBER Cyber Teams (TCTs) of multiple countries can be involved in the test, or one lead authority could be responsible for completing the test, after which it is also valid under the other jurisdictions, as long as the core elements of the involved frameworks and their implementations were followed. Each implementation guide provides some input on this aspect, however making use of different terminology, such as cross-jurisdictional, cross-border, or multi-jurisdictional testing.

> We have executed cross-jurisdictional tests before, which involved multiple TCTs and specific attack scenarios aimed at the CEF of the entity in those particular countries.

Roles, Responsibilities, Deliverables

The TIBER-EU framework has a thorough overview of all involved actors, as well as their responsibilities and deliverables per phase. The specification provides this information in a textual description, in a visual flow per phase, and in table format as part of the Appendix. Not all jurisdiction-specific documents repeat this information and those that do are not always consistent in providing the information in visual, textual, and table format. It is however very useful to include a clear overview to make sure all stakeholders are aware of their responsibilities and major milestones.

> Even though it is not mentioned explicitly, TIBER allows the TI and RT to be performed by the same provider, while maintaining sufficient separation between both teams of course.

Interestingly, in Luxemburg 🇱🇺, the TCT is a cross-institutional team, jointly adopted by the Banque Centrale du Luxembourg (BCL) and the Commission de Surveillance du Secteur Financier (CSSF)

Local Flavours

Besides the items discussed above, which are all based on what is mentioned in the TIBER-EU 🇪🇺 specification, we have also observed jurisdictions adding unique content to their implementation guide. In this section we want to provide an overview of those that we particularly liked or found useful.

The Six Principles of TIBER-DK 🇩🇰

As part of its introduction, TIBER-DK 🇩🇰 has listed six principles that encompass their TIBER mindset and will help participants obtain a successful test:

- Learn & evolve
- Be responsible
- Treat cyber risks as threats to the business
- Be realistic
- Think big and think holistically
- Share experiences

These all support the core objective of TIBER-EU 🇪🇺 to enhance the cyber resilience of the financial sector and are a nice way to set the scene for your guidance document.

TIBER-NL 🇳🇱 as a pioneer

The TIBER-NL 🇳🇱 specification has to be the one with the most local flavour added. They have the longest history with TIBER exercises of course, with TIBER-NL 🇳🇱 laying at the basis of TIBER-EU 🇪🇺.

In terms of Targeted Threat Intelligence (TTI) report, they explicitly mention that it is allowed to update the previous TTI report in case of consecutive TIBER tests, instead of having to create a full TTI report again. This does make sense in case the threat landscape has remained largely the same.

The guide also contains a flow for the formal approval of the red team test plan (RTTP) at three points during the exercise:

- Before the test phase starts
- After six weeks when scenario X is finalized
- After 8 weeks when the detailed plan for the out phase is added and it is finalized

Interestingly, Scenario X is only decided on after 6 weeks of testing and there is an additional detailed plan required for the out phase.

> Formal test plan approval was a suggestion we have provided as feedback to another TCT during a 360 feedback session, as we felt like the red team test plan was of limited relevance after the first submission. It is interesting to see that this was added independently in the TIBER-NL specification.

Another unique piece of information is the (non-exhaustive) list of situations in which the TCT can decide to remove the TIBER-NL 🇳🇱 label of a test, which also means it will not be recognized as a TIBER-XX test in case of multi-jurisdictional testing. In the latter case though, most likely all involved TCTs would agree on revocation of the TIBER label. The guide also mentions what options the entity has in that case; either continuing for the learning experience without being recognized as TIBER test, or consulting with the TCT(s) to determine the necessary steps to still get recognized as a TIBER-compliant test.

Finally, the TIBER-NL 🇳🇱 guide is designed a bit differently, more in a presentation-style format. It also has clickable navigation throughout the PDF, which makes it pleasant to read through.

Optional & mandatory aspects in TIBER-LU 🇱🇺 & TIBER-DE 🇩🇪

In appendix of the TIBER-EU 🇪🇺 guide, there are several tables mapping the mandatory and optional aspects of a TIBER exercise.

TIBER-DE 🇩🇪 summarizes this in their guide with a section titled “Mandatory and voluntary elements” where it explicitly lists a few optional TIBER-EU 🇪🇺 elements that they consider mandatory, as well as points they too consider optional.

> TIBER-DE allows the TI provider to perform light active scanning as well, which can provide additional input for the red team test plan (RTTP). Do make sure not to disclose the exercise due to active scanning though!

TIBER-LU 🇱🇺 adds additional detail by including the same tables as TIBER-EU 🇪🇺 and explicitly mapping which of those items they consider “mandatory and adopted”, “not adopted”, or “optional”, which makes it easy to cross-reference.

RA(S)CI

A summarizing RA(S)CI matrix provides a nice overview of all responsibilities in terms of meetings, deliverables, etc. across the TIBER exercise. Multiple guidance documents (AT 🇦🇹 / BE 🇧🇪 /ES 🇪🇸 / IT 🇮🇹 / LU 🇱🇺 /PT 🇵🇹) include such matrices, usually in appendix. They however don’t all agree on who is responsible for which step specifically, but that is another matter.

One matrix we particularly like is the one added in the TIBER-BE 🇧🇪 guidance, providing a clear list of both meetings and deliverables with detailed RASCI applied to it.

Conclusion

On TIBER

There exists only one TIBER framework, being TIBER-EU, which has been adopted (at the time of writing in July 2024) by 16 countries with national implementations (and the ECB to make 17) that are limited to minor local flexibilities. With the overarching governance of the TIBER-EU guide, the consistency of its implementations is still guaranteed. When working as a provider for different jurisdictions, there may be operational specifics that you will need to adapt to depending on the country. Unless countries maintain their national TIBER implementation for “non-regulated” red teams (which is likely), this may become less relevant considering DORA.

On TLPT

Threat-led Penetration Testing as required by the DORA regulation will be specified in accordance with TIBER-EU and in agreement with the ECB. TIBER can be considered as the “How” to implement the “What” of the DORA RTS on TLPT. Therefore, we expect that by the end of 2024 or early 2025 we will see:

- A more precise TIBER-EU framework reflecting the TLPT requirements
- EU countries publishing updated implementation guides, converging to the updated TIBER-EU framework and DORA regulation – possibly with very minor national caveats. However, we may very well lack country-specific guides and rely on a single European guide.

We will follow-up on this post with an overview of requirements for TLPT and important differences with the existing TIBER-EU specifications. If you already know TIBER-EU, there are some particularly interesting articles in the RTS you may need to be aware of, but things are evolving for the better! Stay tuned!

About the author

Jonas Bauters

Jonas Bauters is a senior manager within NVISO, mainly providing cyber resiliency services with a focus on target-driven testing.
As the Belgian ARES (Adversarial Risk Emulation & Simulation) solution lead, his responsibilities include both technical and non-technical tasks. While occasionally still performing pass the hash (T1550.002) and pass the ticket (T1550.003), he also greatly enjoys passing the knowledge.

Want to know how we can help you with TIBER or TLPT? Visit the ARES team website or reach out directly.

Disclaimer

This blog post was written over multiple iterations, during which certain implementation guides have received updates. The information should be correct at the time of writing (July 2024), but does not come with any guarantees. In addition, certain aspects have been updated based on discussions with members of TCTs, which cannot always be validated through public information/documents.