EUROPEAN CENTRAL BANK

EUROSYSTEM

TIBER-EU

Targeted Threat Intelligence Report Guidance

January 2025

Contents

1 Introduction 2

1.1 Purpose of this document 2

1.2 Target audience 2

1.3 Location within testing process 2

2 Required content of the Targeted Threat Intelligence Report 4

3 Considerations when drafting the Targeted Threat Intelligence Report 6

3.1 Generic Threat Landscape 7

3.2 Collecting threat and targeted intelligence 7

3.3 Considerations when drafting scenarios 10

4 Drafting format 17

5 Annex 18

5.1 Annex 1 – Business overview input 18

1 Introduction

The Targeted Threat Intelligence Report (TTIR) summarizes the findings of the threat intelligence provider (TIP) in regard to the collected threat intelligence and target intelligence as well as describing the scenarios selected for testing as an outcome of the related process step. As such, it provides contextualised intelligence, focusing on the relevant threat landscape whilst incorporating the particular digital footprint and circumstance of the entity. It thereby provides the starting point for the red team testers (RTT) to operationalise the selected threat-led and bespoke attack scenarios to be executed during the tests.

1.1 Purpose of this document

The purpose of this document is to provide the relevant stakeholders with information on the requirements[1] for the content and format of a TIBER-EU TTIR. It also aims at providing guidance on important aspects to be considered during its drafting.

1.2 Target audience

This TIBER-EU guidance for the TTIR is mainly aimed at the TIP, in charge of creating a TTIR in the scope of a TIBER test. Moreover, it supports the control team (CT) and test manager (TM) in assessing the contents of the TTIR. Beyond that, it is useful to read for all stakeholder of a TIBER engagement to understand the nature of its content.

1.3 Location within testing process

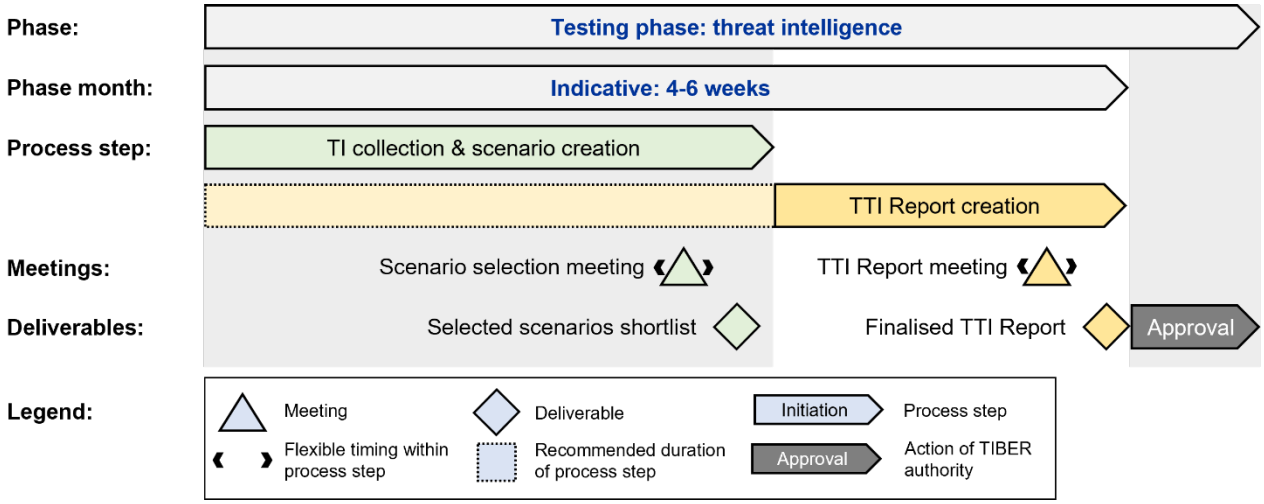
The TTIR is written during the TTIR creation process step of the threat intelligence phase, and finalized after the scenario selection has been concluded.

At the end of the drafting process of the TTIR, on the basis of the selected threat scenarios, the TIP and entity should re-validate the flags set out in the TIBER-EU Scope Specification Document (SSD).

[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]

Threat intelligence collection & Report creation



[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 Required content of the Targeted Threat Intelligence Report

The Targeted Threat Intelligence Report (TTIR) shall include information on all of the following:

- Overall scope of the intelligence research including at least the following:
  - critical or important functions (CIF) in scope;
  - their geographical location;
  - official EU language in use;
  - relevant ICT third party services providers;
  - the period of time over which the research is gathered.
- An overall assessment of what concrete actionable intelligence can be found about the financial entity, such as:
  - employee usernames and passwords;
  - look-alike domains which can be mistaken for official domains of the financial entity;
  - technical reconnaissance: vulnerable and/or exploitable software, systems and technologies;
  - information posted by employees on social media, related to the financial entity, which might be used for the purposes of an attack;
  - information for sale on the dark web;
  - any other relevant information available on the internet or public networks;
  - where relevant, physical targeting information, including ways of access to the premises of the financial entity.
- Threat intelligence analysis considering the general threat landscape and the particular situation of the financial entity, including, at least:
  - geopolitical environment;
  - economic environment;
  - technological trends and any other trends related to the activities in the financial services sector.

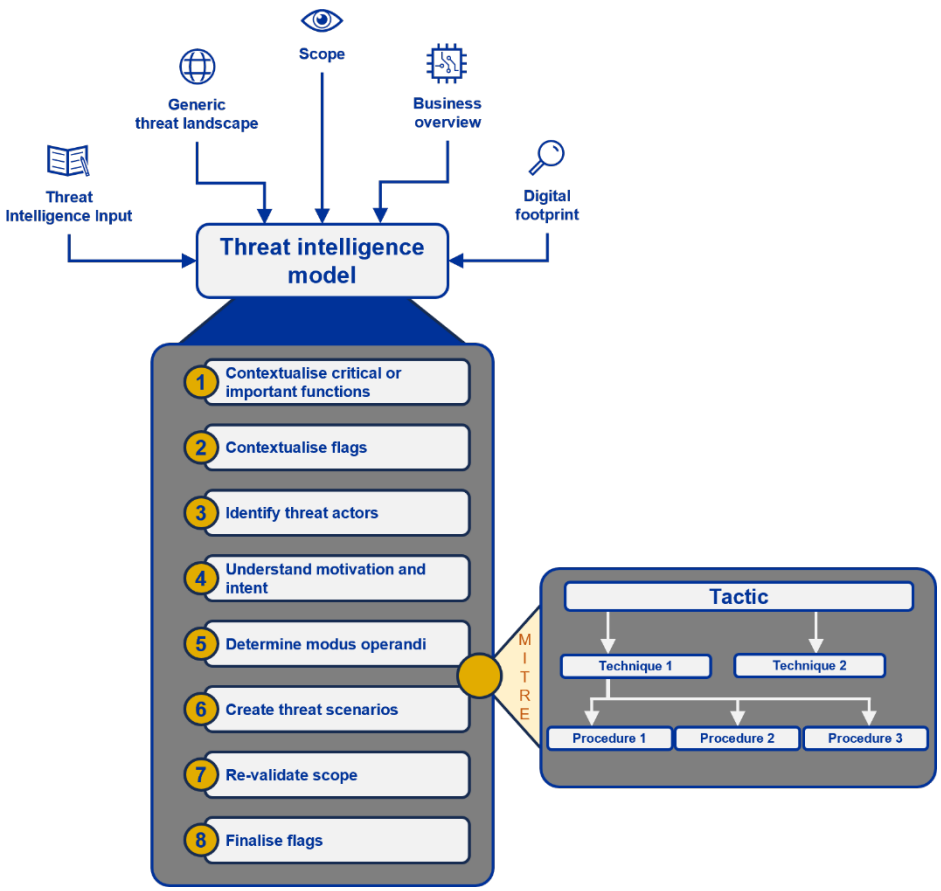
- Threat profiles of the malicious actors (specific individual/group or generic class) that may target the financial entity, including the systems of the financial entity that malicious actors are most likely to compromise or target, the possible motivation, intent and rationale for the potential targeting and the possible modus operandi of the attackers.
- Threat scenarios: at least three end-to-end threat scenarios for the threat profiles identified who exhibit the highest threat severity scores. The threat scenarios shall describe the end-to-end attack path and shall include, at least:
    - one scenario that includes but is not limited to compromised service availability;
    - one scenario that includes, but is not limited to, compromised data integrity;
    - one scenario that includes, but is not limited to, compromised information confidentiality.
- Where relevant, a description of a scenario X.

3 Considerations when drafting the Targeted Threat Intelligence Report

When the TIP develops the TTIR, it should use a variety of methods in intelligence gathering. This may include OSINT (open-source intelligence, which is derived overtly from publicly available sources) and HUMINT (human intelligence, which is derived overtly or covertly from human sources). TIPs must always demonstrate strong ethical behaviour when doing so.

The TTIR should also be shared with the entity's internal cyber threat intelligence (CTI) team after the completion of the TIBER test to help the CTI team validate its own intelligence and reduce the targetable information discovered.

Figure 2
Threat intelligence process in TIBER-EU



3.1 Generic Threat Landscape

In some cases, the jurisdiction implementing the TIBER-EU framework may have decided to produce a national Generic Threat Landscape (GTL) report for the financial sector. The GTL report should elaborate on the specific threat landscape of the country, taking into consideration the geopolitical and criminal threats unique to the jurisdiction.

In cases where the TIBER-XX jurisdiction has developed a GTL, the TIP should make use of it as a foundational knowledge basis in developing the TTIR. If the TIBER-XX jurisdiction has decided not to provide a GTL report, then the TIP should develop a view of the general threat landscape for the entity as part of the TTIR.

3.2 Collecting threat and targeted intelligence

Threat Intelligence refers to the collection, analysis, and dissemination of information about potential or current threats that could harm the entity. It involves gathering data from multiple sources, analysing it to establish patterns and identifying threats.

Targeted intelligence is a subset of threat intelligence focused on threats specifically directed at an organization, its assets, or its personnel. It involves detailed analysis of attacks that are tailored to compromise the particular entity.

During the drafting of the TTIR, analysis of threat intelligence and targeted intelligence alternate and supplement each other.

During the target identification, the TIP should provide a strategic understanding of the entity and what makes the entity an interesting target for active threat actors. TIBER-EU tests are generally conducted on critical financial sector entities, and it is therefore important that the target identification can clearly contextualise how the entity and its CIFs are critical for their sector and/or jurisdiction. This will enable the threat intelligence to be put into context and will contribute to the development of relevant threat scenarios in the TTIR.

3.2.1 Using the Scope Specification Document

At the stage the TIP commences the TTIR, the CT and TM should have agreed on the scope of the test, as documented in the SSD. The TIP should use the information

from the SSD, which outlines the key systems and technologies used by the entity, to collect strategic[3], operational[4] and tactical[5] intelligence.

The TIP should use the CIFs, underlying key systems and services, flags, and the targets and objectives of the test to increase its knowledge of the entity and to focus its threat intelligence for the TTIR. The aforementioned will help inform the TIP on the plausible threat actors targeting the entity and its CIFs, their motivations and modus operandi (i.e. tactics, techniques and procedures) to achieve the flags, targets and objectives. This analysis should be used by the TIP to design the threat scenarios.

3.2.2 Business overview

The entity should provide the TIP with a strategic understanding of the entity's organisation and business, its current and planned activities, and further context of the entity's role within the financial sector. The TIP should use this information to help identify the plausible threat actors targeting the entity and its critical or important functions and to help design the threat scenarios.

Although much of this information can be obtained from open source, it may be more efficient for the entity to provide this information to the TIP, thereby allowing the TIP to focus its efforts on conducting analysis of the information, contextualising it in terms of threat actors, motivations and modus operandi and placing more attention on the digital footprint of the entity.

This information should be shared with the TIP at the start of the threat intelligence phase (see Annex 1). Some of the aforementioned information may be deemed commercially sensitive, and therefore, it important that the entity and TIP engage constructively and take a pragmatic approach during the intelligence gathering phase.

3.2.3 Digital footprint

The TIP, as part of its targeted intelligence gathering, should assess the entity's digital footprint as best as possible. The output of this activity is the identification, on a CIF-basis, of the attack surfaces of people, processes and technologies relating to

[3] Strategic intelligence refers to the contextual framework which shapes an adversary's operating environment and intended course of action. It is designed to explore the 'Who and Why' of an entity's threat landscape.

[4] Operational intelligence involves trend analysis of adversary capabilities and attack methodologies. It is concerned with the 'When, Where and How' of an attack campaign and implies an understanding of adversarial skillset. Analysing an adversary's campaign history allows one to identify characteristic attack vectors and patterns of behaviour that can be used to proactively identify the likely precursors of an impending attack and defend against it.

[5] Tactical intelligence refers to visibility of the tools and hacking methodologies used by cyber adversaries to breach victim networks. High quality, actionable tactical intelligence gives a unique insight into hackers' methods/capabilities and forms the basis for understanding intent at an operator level. It is concerned with the 'How and What' of an attack.

the entity. This includes information that is intentionally published by the entity and internal information that has been unintentionally leaked, such as:

- employee usernames and passwords found on the internet;
- look-alike domains which can be mistaken for official domains of the financial entity;
- technical reconnaissance: vulnerable and/or exploitable software, systems and technologies;
- information posted by employees on social media, related to the financial entity, which might be used for the purposes of an attack;
- information for sale on the dark web;
- any other relevant information available on the internet or public networks;
- where relevant, physical targeting information, including ways of access to the premises of the financial entity.

The TIP should use this information to help identify the plausible threat actors targeting the entity and its CIFs and to help design the threat scenarios.

The TIP may use OSINT, information provided by the entity, the dark web and closed sources, to gather information about the entity's digital footprint. When gathering intelligence on the digital footprint of the entity, it is critical that the TIP does not conduct any activity which alerts the blue team and reveals that a TIBER test is being performed. Active reconnaissance can be performed by the RTT in the TI phase as relevant, at the request of the TIP and after approval of the CT and TM.

3.2.4 Intelligence input

In gathering the appropriate tactical and operational intelligence, to help inform the threat scenarios, the TIP should at least consider geopolitical and economic environment as well as technological trends amongst other developments relevant for the financial services sector and take into account the following:

What information can be found that threat actors would use to better understand the target network environment, specifically the CIFs and systems underpinning it?

- What information could be found from network diagrams (if available) that could assist attackers in determining where CIFs are located within the network and any interconnected systems and secure connections to CIFs?
- What information about the systems underpinning the CIFs is available that reveal potential vulnerabilities that could be exploited by actors?
- Which components of the network infrastructure of the entity have been targeted by selected threat actors before?

- What are the most prevalent and/or critical vulnerabilities for the sector that are likely to be present at the entity?

  What information would threat actors be able to obtain in order for successful social engineering to be performed to gain initial access to the infrastructure (when applicable in the scenarios)?

- What personnel could be targeted by threat actors based on the job roles and assumed levels of privileged access to key technologies or CIFs?
- What contact details and credentials belonging to key personnel can be found that could assist threat actors in their attacks?

  How do third parties/managed service providers affect the security posture of the entity, and how would these parties be used by threat actors to attack the entity?

- Which of the entity's third-party/managed service providers have been compromised before and how could this provide opportunities for actors to compromise the entity?
- Which of the entity's third-party/managed service providers could be compromised and how could this provide opportunities for actors to compromise the entity?

In general, the TIP should use information related to the scope, business overview, digital footprint and intelligence input in an interconnected manner, as they inform and influence each other, and provide a broader and holistic picture of the entity's threat landscape – these components should not be analysed in silos.

3.3 Considerations when drafting scenarios

Once the TIP has gathered sufficient threat and targeted intelligence, they should use it to help develop the threat scenarios, in line with the **'TIBER Threat Intelligence Model'** set out in Figure 2 as an eight-step approach.

3.3.1 Contextualise critical or important functions

The information gathered should provide the TIP with more detailed background information on the entity and provide the basis for further contextualisation of the CIFs set out in the SSD. For example, the SSD may list the CIFs as below:

CIF	Sub-categories	Justification for inclusion
Deposit taking and savings	Current accounts	Deposit taking and savings services are a core function for the real economy, and any disruption to these would have a detrimental impact on the customer base. Customers of a disrupted deposit taker may lose immediate access to their deposits, and thus are not able to execute payments. In the event of disruption to a significant deposit taker, the resulting liquidity shortage could have serious adverse effects on activity in the wider economy.
	Savings accounts	
	Retail internet banking	
	Debit cards	
	ATM cards	
	Credit cards	
	Mortgages	
	Home equity loans	
	Personal loans	

The information gathered from the GTL, business overview, digital footprint and threat intelligence input should enrich the understanding of the TIP and provide more robust, specific intelligence to determine the threat actors that would target the critical or important functions and their modus operandi.

3.3.2 Contextualise flags

The information gathered should provide the TIP with more detailed background information on how threat actors would target the entity's CIFs and focus their efforts on achieving the objectives/flags, as set out in the SSD.

The SSD lists the CIFs, their underlying systems and services, and the objectives/flags that the RTT will look to compromise. The information gathered helps inform the TIP with more specific details how the threat actors would look to compromise the critical or important functions, the underlying systems and services and achieve the objectives/flags. The TIP should incorporate this specific information in the TTIR to contextualise the flags by developing more concrete threat scenarios that will allow the RTT to build the attack scenarios and help compromise the flags/objectives during the test.

For example, the digital footprint may provide the TIP with important information from staff profiles on social media, or the threat intelligence input could reveal vulnerabilities related to the underlying systems and services, which could be used to exploit the entity.

It should be noted that finalising the flags constitutes a fluid process, and whilst the TTIR helps inform this, flags can be changed on an iterative basis in the Red Team Test Plan (RTTP) and during the active testing.

3.3.3 Identify threat actors, understand capability and intent

The information gathered on the contextualised CIFs and flags should allow the TIP to conduct its own assessment on which threat actors are relevant for the entity. The TIP should list the categories of threat actors and threat actors ranked by intent and capability to attack the entity and/or a specific critical or important function of the entity.

The assessment of the TIP should be based on specific actors. The TIP can firstly use a categorisation of threat actors, and assess how each of these categories relates to the entity. When the categories are assessed and listed, then the TIP should determine which threat actors are deemed most relevant to the entity and why.

For each of the threat actors listed, the TIP should provide analysis on their motivations and intent, and explain clearly why they would specifically target the CIFs and attempt to achieve the objectives/flags. This analysis must be evidence based and demonstrate strong analytical reasoning in terms of motivation and intent. For example:

"APTXX has long targeted European countries. It is strongly believed to be operating for country X. In recent years tensions have risen between country X and European countries which has led to a rise of disruptive operations against critical infrastructure in Europe. Until recently these operations were limited to non-financial sector. However in June this year the central payment processor neighbouring country Y was target of APTXX and caused an outage of two weeks.

After this successful operation APTXX has been ordered by country X to investigate whether they can find a way into European payment institutions in order to shut down operations when geopolitical tensions rise even further. They are likely to use both physical and digital means, as shown by incidents 1 and 2 in Europe this year."

During these steps, the TIP can map the threat actors to the CIFs as identified in the SSD and the underlying motivation and intent. For example:

	CIF 1: Asset management	CIF 2: Payment processes	CIF 3: Processing of PII
Name actor 1 (Organised Criminal Group)	Financial gain – Theft of Money	Financial gain – Fraudulent transfers	Financial gain – Theft and selling of PII
Name actor 2 (Organised Criminal Group)	Financial gain – Theft of Money, Theft and selling or use of Market sensitive information	Financial gain – Theft of Money	Financial gain – Theft and selling of PII
Name actor 3 APTxx (Nation State)	Espionage – Theft of confidential information		Espionage – Monitoring Opponents

Furthermore, the TIP should also provide an explanation as to why other (categories of) threat actors are excluded.

3.3.4 Determine modus operandi

Once the TIP has adequately linked the CIFs, flags, threat actors and their capability and intent, based on the evidence gathered during the reconnaissance, they should determine the modus operandi, including TTPs, that the threat actor would employ to compromise the CIFs and achieve the objectives/flags.

It is important that the TIP sets out a detailed analysis of the TTPs that the real-life threat actor would use – in this regard, the TIP uses the latest **MITRE ATT&CK framework** as the model[6] to develop threat scenarios.

The MITRE ATT&CK framework sets out detailed and prescriptive TTPs, and provides a robust and comprehensive basis for the TI/RTTs to plan the threat and attack scenarios. The TIP should map the CIFs, objectives/flags and threat actors to the TTPs that would most likely be used by the real-life threat actor. For example:

[6] https://attack.mitre.org/

Threat actor	Objective/flag	Tactic	Technique	Procedure(s)
APTxx (Nation State)	**Exfiltration of sensitive data**	**Exfiltration** - The adversary is trying to steal data.	**Automated Exfiltration** - Data, such as sensitive documents, may be exfiltrated through the use of automated processing or Scripting after being gathered during Collection.	**Machete** - Machete's collected files are exfiltrated automatically to remote servers. **USBStealer** - USBStealer automatically exfiltrates collected files via removable media when an infected device is connected to the second victim after receiving commands from the first victim

Whilst this provides a good basis for the test, the RTT should be flexible and ready to change course during the test and apply other TTPs.

3.3.5 Create threat scenarios

Based on the information gathered and the analysis undertaken, the TIP should clearly document the threat scenarios for the TIBER test. First in the form of high-level scenarios for a longlist, after which at least three scenarios are chosen. The number of threat scenarios in the longlist will differ by test, depending on the nature of the entity, the scope, flags and the overall information gathered during the reconnaissance. However, the proposed scenarios should target each and every CIF in scope of the test, and should be sufficient to stimulate a substantiated debate between the CT and TM. Generally, a longlist of at least six scenarios should be expected.

The high-level scenarios for the longlist do not need to be expanded in full detail. However, they should be built based on the detailed reconnaissance of the information, focusing on the specific intent of the threat actor for attacking a specific CIF of the entity in scope of the test, and taking into account what TTPs a threat actor would employ when attacking the entity.

The threat scenarios should not be based on historical data only. Rather, the TIP is also expected to consider and analyse where the threat actor will go next and what new avenues the threat actor is likely to explore. The TIP can use its creative

freedom and knowledge of developments to forecast upcoming attacks for the selected threat actors. The TIP should also take into account:

- the sophistication of techniques the actor would use;
- the agility of the threat actors (i.e. how the threat actor would adapt quickly to changing circumstances and how would they do this);
- how targeted they are towards their end goal (i.e. do they go directly to the CIF or firstly provide broad presence within the network and/or roam around to look for opportunities); and
- their knowledge of the financial sector, its functions and the systems being used (i.e. have they targeted the financial sector or similar systems before).

The threat scenarios shall describe the high-level end-to-end attack path and shall include, at least:

- one scenario that includes but is not limited to compromised service availability;
- one scenario that includes but is not limited to compromised data integrity;
- one scenario that includes but is not limited to compromised information confidentiality.

Although not all CIFs in the scope need to be targeted in the scenarios shortlist, there should be breadth and depth in the CIFs targeted. Out of the longlist the CTL should select at least three scenarios to conduct the test, the selection of which should be based on at least the following elements:

- The recommendation of by the TIP and the threat-led nature of each scenario.
- The input provided by the TTM.
- The feasibility of the proposed scenarios for execution, based on the expert judgement of the testers.
- The size, complexity and overall risk profile of the financial entity and the nature, scale and complexity of its services, activities and operations.
- Only one of the selected scenarios may be non-threat-led and may be based on a forward-looking threat, with high predictive, anticipative, opportunistic or prospective value. Such scenarios are also known as ‘scenario X’ and may include hybrid, novel TTPs and “out of the box” elements. The scenario X should be based on anticipated developments of the threat landscape, customised to the entity.
- In case of a multi-party test involving an ICT third party provider, at least one of the selected scenarios should cover the ICT third party providers’ systems, processes and technologies supporting the CIFs of the entities in scope.

Other substantial factors to consider when selecting the scenarios are:

- the sophistication of the threat actor (more versus less advanced actors);
- the noise that the scenario will create, potentially impacting the order of execution of the scenarios;
- the different motivations and intent from the actors;
- any learning goals that the entity has defined for the test.

After this selection is done, the scenarios on the shortlist should be worked out in more detail, combining the previously gathered information, including a narrative, and detailed attack path including references to MITRE TTPs. If a scenario X has been selected, a degree of flexibility should remain so that the details can be decided on during the RT phase.

4 Drafting format

The TIBER-EU TTIR may be drafted in any preferred format, provided that all required information is included. All content that needs to be provided in order to complete this document is indicated in Chapter 2. Example templates (if any) to be used on a voluntary basis are provided in the annex.

5 Annex

5.1 Annex 1 – Business overview input

Before commencement, the entity should, at a minimum, provide the TIP with the following:

- an explanation of the entity and its critical or important functions and their significance for the broader financial sector;
- the entity's own threat assessment including examples of recent adverse cyber events;
- the potential systemic implications of a compromise in confidentiality, integrity and availability of the entity;
- information about the entity's business model, its organisational setup (e.g. shareholder ownership, company structure and Board and executive management), its products and services and its key financial figures;
- the countries in which the entity has presence;
- information about the entity's interdependencies (i.e. financial and operational) and disclosure of countries from which the entity receives (significant) supply chain support (e.g. IT support is outsourced to country X);
- the types of clients that the entity has, which might be of interest to foreign intelligence agencies - characteristics of these clients could be shared by the entity without mentioning specific names;
- the niche markets in which the entity is active;
- high level insight on any niche Research and Development knowledge or Intellectual Property of the entity;
- high level insight on possible (future) mergers and acquisitions (M&As) of the entity which may increase the interest of certain threat actors;
- high level insight on geopolitical issues related to the entity or investments by the entity, which may impact its threat landscape;
- details of third-party involvement in critical or important functions; and
- details of the entity's domains and IP addresses.

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