ART Threat Intelligence Guide

for the financial sector

DeNederlandscheBank

EUROSYSTEEM

Contents

1 About this guide

2 Introduction

3 Core principles of Threat Intelligence

4 Threat Intelligence variants

5 Description of the threat intelligence steps

6 Overview of the provider requirements

Annex

1 About this guide

This document first provides a short introduction to Threat Intelligence (TI) in ART. This is followed by a description of the core principles of TI, highlighting options, objectives and purposes in the TI module. Next, the different TI variants and their requirements are described. Finally, the steps in planning, preparing, executing and evaluating are described for every TI variant. For a list of abbreviations, see annex A.

1.1 Purpose of this guide

In every ART test, TI is a mandatory part of the test. In line with the modular approach of ART, the framework offers financial institutions three distinctly different TI variants. In consultation with the Test Cyber Team (TCT), institutions can select a variant that best fits the learning objectives and maturity of their organisation. Every variant has its own set of (minimal) requirements, process steps, and stakeholders involved. This TI guide will explain what every variant entails, what the requirements are, who should be involved and what the steps are towards creating a threat intelligence report (TIR) that meets all specified criteria.

This guide is part of the ART framework as published by De Nederlandsche Bank (DNB) on ART-NL | De Nederlandsche Bank | De Nederlandsche Bank (dnb.nl). For enquiries about ART, please contact the DNB Test Cyber Team (TCT) at tct@dnb.nl.

1.2 Target audience

This guide is intended for control teams (CTs) who are responsible for the ART test in the financial institution and for selecting an appropriate TI variant. Additionally, this guide is intended for the Threat Intelligence provider (TIP) who is responsible for executing the TI phase of the test and producing a TIR.

1.3 Legal and disclaimer

This document is intended for institutions within the scope of an ART test. Nothing in this guide should be construed as legal or professional advice. This guide is an underlying document of the ART framework. For information on copyrights and creative commons, please refer to Section 1.3 of the ART framework.

1.4 Role of the TCT, minimum requirements and attestation

To make sure the quality of the test meets the ART standards, TCT-DNB will be present throughout the execution of the TI module (and the other modules). The TCT is involved to ensure that the TI module is prepared, executed and evaluated following the requirements as presented in this guide. At critical moments in the module, the TCT provides a go/no go on certain deliverables, such as the TIR. The TCT will work in close collaboration with the Control Team (CT) and the TIP.

Next to the quality assurance (QA) role, the TCT is a neutral sparring and guiding partner for the Control Team Lead (CTL) who holds the ultimate responsibility for the ART test within the institution, and for the TIP project team.

If the test has been carried out in accordance with the requirements of the ART framework, the TM will provide the institution on behalf of the TCT with a DNB attestation document concluding the test.

2 Introduction

This section describes what TI is and why it is included in the ART framework. It also discusses the purpose and target audience for TI.

2.1 What is the Threat Intelligence module in ART?

Ethical hacking frameworks like ART differ from standard red team tests by the fact that the attacks on the institutions' system during an ART test must be built on accurate and tailored threat intelligence. This makes the test more realistic and the outcomes more valuable for the financial institution when assessing its cyber resilience and when drafting the plan.

This accurate and tailored threat intelligence report is drafted by a TIP during the TI phase. The TIP uses a wide variety of open and closed sources and several analytical methods to determine the most pressing threats and vulnerabilities for the financial institution. Based on this information, the TIP develops a number of realistic scenarios that will be used by the RTP to formulate their RTTP.

The final deliverable of the TI phase is a TIR that is approved by the TCT and CT.

2.2 What is the purpose and goal of Threat Intelligence?

The purpose of the TI phase in ART is twofold. First, accurate and insightful TI research, followed by a TIR, can provide a financial institution with new insights and a fresh perspective on the cyber threats and potential vulnerabilities it faces. Second, a comprehensive TIR gives the red team a solid foundation of credible and reliable TI scenarios on which they can build their RTTP. These two purposes can deliver the following results for the institution:

1. The institution will have a better understanding of the threats and vulnerabilities it has to arm itself against.
2. The institution will have a better understanding of how its cyber defences hold up against a realistic cyberattack.
3. Test results can significantly influence the management board's decisions regarding resource allocation when they realise that 'this could have happened to the organisation in real life'.

In addition to these learning objectives, the formal objective is to achieve approval by the TCT and CT on the TIR so that the test can advance to the RT phase.

2.3 What is the Generic Threat Landscape (GTL)?

An important component of every TI phase is the Generic Threat Landscape (GTL). The GTL is specifically designed by the TCT for financial institutions that perform an ART or TLPT/TIBER test. Every participating institution will be provided with a copy of the most recent GTL by the TCT at the beginning of the test.

The GTL provides information about advanced threat actors that are relevant to Dutch financial institutions, as well as exploring those actors' motivations to attack specific critical or important functions (CIFs) within these institutions. It also includes various scenarios that can provide inspiration for the TIR and/or the red team test plan (RTTP). However, it is important to emphasise that the scenarios are only included in the GTL as examples and should not be used in the final version of the TIR without modification, verification or expansion. Depending on the variant selected in ART, the GTL serves as primary input for the TIR report.

The GTL contains the following elements:

1. A strategic geopolitical overview of the most relevant cyber threats for the Dutch financial sector.
2. The most relevant cyber threat actors for the Dutch financial sector.
3. An overview of CIFs within Dutch financial institutions that fall within the scope of ART.
4. Threat matrices outlining the motivation and intent of cyber threat actors to conduct attacks against the various CIFs outlined in the GTL.
5. Sample scenarios that could help a CT, TIP or RTP to develop the scenario(s) for their ART engagement.

3 Core principles of threat intelligence

This chapter describes the core principles of the TI module in an ART test. These core principles provide the reader with a clear understanding of the key notions, ideas and concepts that are essential for conducting the TI module.

- **Safety and a safe learning environment** – For all ART modules, the most important rule is that safety and a safe learning environment come first. Depending on the thoroughness of the selected variant, the TI phase may uncover critical vulnerabilities or access points into the institutions' system that the institution is not yet aware of. When such a vulnerability is discovered, or when in doubt, the TIP will always confer with the CTL and TCT whether this vulnerability needs to be addressed immediately or that it can be used during the RT phase. The CT and TCT must have sufficient confidence in safety, capacity and expertise of the TIP. The balance between an impactful TIR with plenty of leads for the RT on the one hand and ensuring that significant threats are not permitted to persist for an extended period on the other needs to be decided in close collaboration with the TIP, TCT and CT.

- **Scenario selection is aligned with the learning goals...** – The learning goals defined in the preparation phase of the ART test run as a common thread throughout the entire engagement. Although the TI collection and analysis phase is separate from the learning objectives, these objectives ultimately influence which scenarios are built and selected.

- **... but also independent from organisational restriction**s – It is also possible that the TIP discovers information about the institution that is not in scope of the learning objectives defined by the institution. Nevertheless, such information can still be useful for potential (out of the box) RT scenarios and will be included in the TIR. For example: if a financial institution has excluded third parties from the scope but the TIP discovers a critical third-party vulnerability, this will be included in the TIR.

- **Timeliness, actionability and relevance** – During the threat intelligence phase, it is essential that collected information remains relatively up to date. The more recent the intelligence, the greater its capacity to meaningfully impact the scenarios. At the same time, the intelligence must be actionable, either directly or indirectly, to enable the red team to effectively use it when developing and executing the RTTP. Finally, the TIP must clearly demonstrate how the intelligence it has gathered is relevant to the financial institution being tested.

- **The TI phase is always passive** – Reconnaissance during the TI phase is always passive. Even though active reconnaissance can lead to valuable additional information, there is also a substantial risk that active scanning will be noticed by the institution's blue team (BT). As a result, the RT phase could be compromised before it even starts. Passive reconnaissance involves gathering information without directly interacting with the target, using publicly available sources such as websites, social media and leaked data. It is discreet and minimises the risk of detection. Active reconnaissance, on the other hand, requires direct engagement with the target's systems or infrastructure, such as scanning networks or probing services. While active methods provide more detailed insights, they carry a higher risk of being detected and triggering defences.

- **Conducted by experienced professionals with demonstrable experience** – Searching, analysing and reporting TI requires specialised expertise and should therefore be conducted by professionals. These professionals must have relevant experience and be able to collaborate effectively with the RTP and internal organisation. Requirements vary per TI variant. More about the requirements for staffing and procurement

can be found in Chapter 5 of this document and in the ART Service Procurement Guidelines.

- **Confidentiality** – Confidentiality is essential during all ART modules, including TI. The organisation should not become aware of the ART test because of an information leak in the TI phase. For example: internal experts may be consulted about the institution's CIFs during the TI phase. These experts should keep all dealings concerning the test secret for the duration of the engagement. If unauthorised employees of the institution find out that the TI phase is underway, this could compromise the entire ART test.

4 Threat Intelligence variants

This chapter describes the different TI variants that can be chosen during an ART test. It provides a brief overview of the pros and cons of each variant and explains which types of tests and organisations they are best suited to.

4.1 Introduction and overview

RT scenarios that are based on actionable and realistic TI are a powerful tool for testing and enhancing a financial institution's cyber resilience.

However, the scope and nature of the TI module should always align with the learning objectives, resources and maturity of the institution being tested. In line with the modular approach of the ART framework, the TI module comprises three variants. While none of these variants are inherently superior to the others, they do produce different results and require different resources. Therefore, it is important that the CT, in close coordination with the TCT, chooses the variant that best fits the institution. The variants are: 1. Basic TI, 2. Extended TI and 3. Full TI. The major similarities and differences are shown in the table below.

	Basic	Extended	Full
Purpose	Provides a basic understanding of the cyber threat landscape and the institution that can serve as strategic input for one RT scenario.	Provides a broader understanding of the cyber threat landscape and the institution. It includes multiple threat actors and scenarios that can serve as strategic input for multiple RT scenarios.	Provides a thorough analysis of the cyber threat landscape and the institution. This includes targeted threat intelligence that can be used as operational input for multiple RT scenarios.
Complexity	Low	Medium	High
Relative investment	Low	Medium	High
Potential value	Medium	Medium	High
Average duration	2-4 weeks	4-6 weeks	≥6 weeks
Can be performed by	Internal team, RTP, TIP	Internal team, RTP, TIP	RTP, TIP
Deliverable	Basic TIR (5-10 pages)	Extended TIR (10-20 pages)	Full TIR with the addition of targeted threat intelligence (≥20 pages)
Best suited for	Smaller institutions that conduct their first ART test with one RT scenario, or larger institutions that conduct a smaller ART test in between TLPT tests.	Institutions that have already done a previous ART test and/or institutions with more TI capacity to process the contents of the TIR.	More mature institutions that are working towards a TIBER test and/or are conducting an ART test with multiple RT scenarios.

4.2 Variant 1: Basic TI

What should a basic TIR include?
The deliverable at the end of a Basic TI is a TIR (5-10 pages). This TIR should include at least the following elements:

1. An executive summary of the most likely threats and the scenarios that should be tested.
2. A business overview of the financial institution being tested, including relevant CIFs.
3. An overview of the cyber threat landscape relevant for the institution.
4. A limited amount (+/- 3) of threat actors corresponding with the identified threats. A brief description, motivation and MO for each of the actors must be included.
5. An analysis of the elements above resulting in at least 1 TI-based scenario.

Sources of a basic TIR
The foundation of a basic TIR is the GTL provided by DNB and the institution's Scope Specification Document (SSD). These two sources should at least be supplemented by open-source intelligence (OSINT) information collected by the (internal) TIP. Additionally, any recent TIRs that the institution already has can be used as source of inspiration. The DNB-TCT generally considers a validity period of 24 months for any current or previously issued TIR. The CT and the external TIP may hold an optional information exchange meeting, in which the CT explains the CIFs in scope and corresponding business functions in more depth. All the information listed above should be analysed and processed, so that the final result explains (1) how the different sources fit together, (2) which information is relevant for the test and why, and (3) how the information fits into a logical report.

Who can produce a basic TIR?
A basic TIR can be produced by various threat intelligence experts/providers. If the institution that is being tested has sufficient internal TI capacity, as described in Chapter 6, this department/these people can produce the basic TIR. The same applies to the RTP. If they have internal TI capacity/an internal TI expert, the RTP can most likely also produce this type of report. The final option is a dedicated external TIP. They have the most expertise, but it is less likely that a dedicated TIP will take on such a limited assignment.

For more information on who can produce a basic TIR, please see Chapter 6.

For whom is a basic TIR?
A basic TIR is best suited for institutions:

1. With limited capacity to process threat intelligence AND/OR
2. That conduct an ART test with only one RT scenario AND/OR
3. That have recently conducted another ART/TIBER test with full TI AND/OR
4. With relatively limited resources AND/OR
5. That are conducting an ART test for the first time.

Pros and cons

+ Relatively cost-efficient.
+ Easy to digest for smaller organisations.
+ Can be conducted by various TI experts/providers.

– Only scratches the surface of the threat landscape.
– Has limited value for the subsequent RTTP.
– No targeted threat intelligence.

4.3 Variant 2: Extended TI

What should an extended TIR include?
The extended TI variant is a more advanced version and requires more resources and expertise. It may also add more value to the RT phase and the institution. The deliverable at the end of an Extended TI is an extensive TIR (10-20 pages). This TIR should include at least the following elements:

1. A summary of the CIFs of the institution, the most likely threats, the corresponding actors and the scenarios that should be tested.
2. A business overview of the financial institution that is being tested, including relevant CIFs.
3. An overview of the cyber threat landscape, highlighting and explaining the cyber threats relevant for the institution.
4. A limited amount (+/- 5) of threat actors corresponding with the identified threats. A description, motivation and MO for each of the actors must be included.
5. An analysis of the elements above resulting in at least 3 TI-based scenarios.

Sources of an extended TIR
Similar to the basic TIR, the GTL and the SSD form the foundation of an extended TIR. However, the extended TIR puts far more emphasis on additional own resources and analysis by the TIP. The TIP is expected to do a deep dive in the institution itself, the threat landscape and the potential actors interested in the institution. Although not mandatory, the use of an 'own' TI platform by the TIP is highly encouraged. It is highly recommended that the CT and the TIP hold a business overview workshop. In this optional information exchange meeting, the CT explains the CIFs in scope and corresponding business functions in more depth. Any recent TIRs that the institution already has produced or obtained can also be used. These TIRs should not be older than 24 months. All the information listed above should be analysed and processed so, that the final result explains (1) how the different sources fit together, (2) which information is relevant for the test and why, and (3) how the information fits into a logical report. Since an extended TIR is roughly double the size of a basic TIR, the TIP has more room and responsibility to explain their line of reasoning and to corroborate and elaborate on their statements, claims, analysis and scenarios.

Who can produce an extended TIR?
An extended TIR can be produced by various threat intelligence experts/ providers. If the institution that is being tested has sufficient internal TI capacity, this department/these people can produce the extended TIR. However, compared to the basic TIR, internal experts are held to a more demanding standard. The extended TIR can also be produced by the contracted RT if they meet the requirements. The final option is a dedicated TIP.

For more information on who can produce an extended TIR, please see Chapter 6.

For whom is an extended TIR?
An extended TIR is best suited for institutions:

1. With capacity to process threat intelligence
2. That conduct an ART test with one or two RT scenarios.
3. With a limited understanding of their strategic threat landscape.
4. That are conducting their first or repeated ART test.

Pros and cons

+ Offers more in-depth insight compared to the basic TIR.
+ Provides the CT with several options/scenarios for the RT phase.
+ Still relatively easy to digest for smaller organisations.
+ Can be conducted by various TI experts.

– More resource-intensive compared to a basic TIR.
– Has limited value for the subsequent RTTP due to the lack of targeted threat intelligence.
– For institutions that have a Security Operations Centre (SOC), an extended TIR offers limited value for mitigating operational threats.

4.4 Variant 3: Full TI

What should a full TIR include?
The full TI variant is the most extensive threat intelligence version in an ART test. This variant is similar to the TI phase in a TLPT/TIBER test. Only a TIP with extensive knowledge, experience and resources can produce a full TIR. Consequently, this is also the most resource-intensive option for the financial institution. The added value for the financial institution for choosing this variant is that it will get an extensive and comprehensive overview of its own critical functions, its vulnerabilities and threat actors that are interested in these. A full TIR includes an additional dedicated targeted threat intelligence section with operational intelligence on vulnerabilities and threat actors. This information can be used directly by the RT. The deliverable of the full TI variant is a comprehensive report (at least 20 pages, but likely more, due to the volume of targeted threat intelligence). Based on previous experiences an average report will likely be between 50 and 100 pages. This TIR should contain at least the following elements:

1. A summary of the CIFs of the institution, the most likely threats, the corresponding actors and the scenarios that should be tested.
2. A business overview of the financial institution that is being tested, including relevant CIFs.
3. An overview of the cyber threat landscape, highlighting and explaining the cyber threats relevant for the institution.
4. A longlist (≥10) of threat actors corresponding with the identified threats and with diversity of threat scenarios in mind.
5. A shortlist of threat actors (+/- 5) derived from the longlist. This shortlist explains why these actors are the most likely to attack the financial institution, detailing their MO and their most commonly used TTPs.
6. For every CIF identified in the SSD, the TIP should create a brief scenario.
7. Based on this longlist of scenarios, a shortlist of at least three scenarios is created. The shortlist explains these scenarios in detail and provides technical information on the selected threat actor(s). These scenarios should at least include: (1) a narrative, (2) in, (3) through and (4) out.
8. A section with targeted threat intelligence on the institution itself and targeted threat intelligence supporting the scenarios on the shortlist.

Sources of a full TIR
As with the other two variants, a full TIR 's starting point is the SSD provided by the financial institution. Another similarity is that a full TIR can draw information from the GTL. Unlike the basic and extended variants, the GTL is a source of inspiration rather than the main source of information. The focus should be on the TIP's own OSINT, own TI platforms and own Dark Web research. It is highly recommended that the CT and the TIP hold an information exchange meeting, in which the CT explains the CIFs in scope and corresponding business functions in more depth. Any recent TIRs that the institution already has produced or obtained can also be used. These TIRs should not be older than 24 months.

All of the information listed above should be analysed and processed, so that the final result explains into a logical and detailed way (1) how the different sources fit together, (2) which information is relevant for the test and why and (3) how the technical/operational intelligence supports scenarios that are drafted in the strategic intelligence section. Since the full TIR is virtually a blank cheque in terms of document size, the TIP is responsible for comprehensive reporting while ensuring the document remains concise and focused.

Who can produce a full TIR?
A full TIR can only be produced by specialised threat intelligence providers: an RTP with sufficient qualifications and experience and a dedicated TI provider. The full TI variant cannot be produced by an internal TI team. Even if the institution's internal threat intelligence capacity matches a professional provider's standards, it is mandatory to use an external TIP to gain a fresh perspective and maintain independence from the financial institution. This means a full TIR could potentially also be produced by the RT provider, but only if its qualifications, capacity and experience are in line with the requirements set out in the ART Service Procurement Guidelines and match those of a specialised TIP. Similar to TIBER, a full TIR can be produced by specialised TI provider.

For more information on who can produce a full TIR, please see Chapter 6.

For whom is a full TIR?
A full TIR is best suited for institutions:
1. With a mature capacity to process operational threat intelligence AND/OR
2. Institutions that, in the recent past, have not yet commissioned a complete TIR AND/OR
3. That conduct an ART test with at least two RT scenarios AND/OR
4. That have an extensive understanding of their strategic and operational threat landscape.

Pros and cons
+ Offers the most in-depth insight of all TIR variants.
+ Provides the CT with several options/scenarios for the RT phase.
+ Provides the institution with actionable intelligence to improve its defences.
+ Provides operational input for the RT phase.

– The most resource-intensive and expensive TIR-variant.
– Not for organisations who do not have the capacity to process operational or even technical intelligence.
– Even a well written/structured full TIR may produce an overwhelming amount of information for a financial institution. A less well written/structured report amplifies this effect.

4.5 Which module to choose?

During the preparation phases, the CTL and the TCT meet to discuss the scope of the ART test and to decide which modules and variants to include. The decision as to which modules to include in the ART test ultimately lies with the institution itself.

The same applies to the type of threat intelligence provider the institution intends to engage. The considerations below, along with those in Chapter 6, should influence the TIP selection. Ideally, the choice of TIP and the choice of a specific TI variant should be aligned. See Chapter 6 for more details about this alignment.

The TI module is mandatory under the ART framework, but it is up to the financial institution to select a variant. Which variant is the best fit for any specific ART test depends on the following considerations:

- **TI capacity within the financial institution**
  Financial institutions with substantial internal TI capacity are generally better equipped to deal with extensive and complex TIRs. Smaller institutions with less TI capacity tend to benefit less from such detailed reports. The size and maturity of an institution are important factors to consider when selecting the appropriate variant.

- **Learning objectives of the institution**
  The choice of a TI variant is directly linked to the institution's learning objectives in the test. When these objectives also involve threat intelligence, a more advanced TI variant is recommended. For example: if the institution is interested in learning which of its vulnerabilities are exposed on the internet, then the Full TI variant might be of more added value to them than the Basic or Extended TI variant.

- **Alignment with the other modules of the ART test**
  The TI variant selected should align with the scope of the other modules. For example: if the RT phase consists of only one scenario with an assumed compromise, a full TIR might be an overkill for that purpose.

- **Financial resources**
  Larger TI variants tend to be more expensive, so institutions with limited budgets may opt for a smaller TI variant.

- **Previous experience with TIRs**
  If the institution produced or obtained a TIR on its environment and threat landscape within the past 24 months, the likelihood of obtaining new information from another TIR is limited. Both the institution's systems and the external threat landscape do not change that much over this relatively limited amount of time. In such cases, a smaller TI variant is recommended.

5 Description of the threat intelligence steps

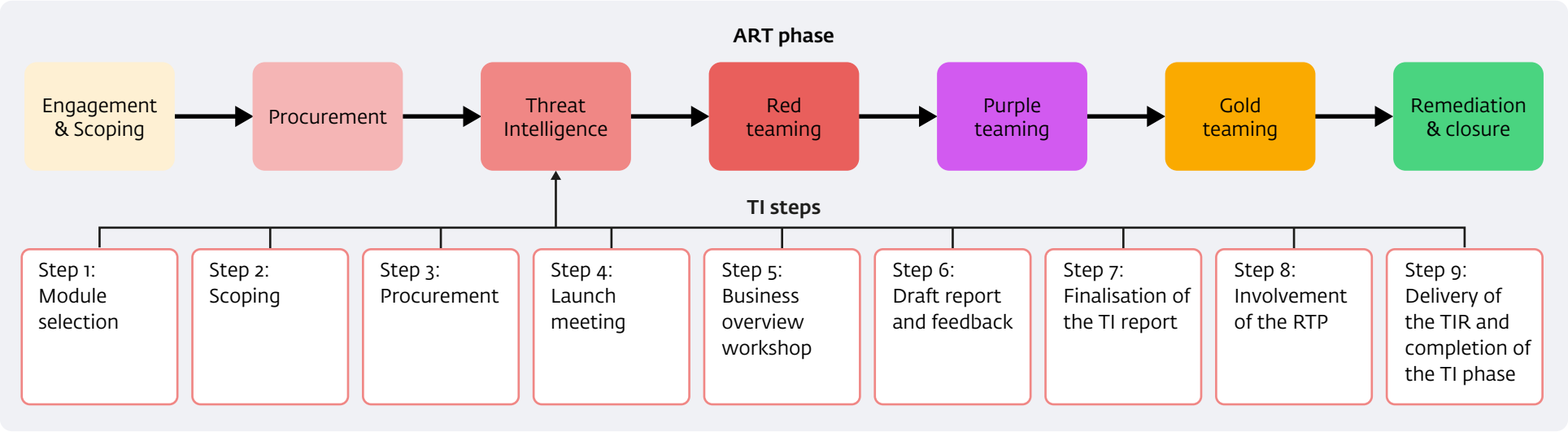
This chapter provides a step-by-step guide for the TI phase, outlining the milestones, deliverables and required meetings.

5.1 Steps for all variants related to the threat intelligence phase

Although the TI module offers three variants, the processes for producing the TIR are largely similar for all three of them. Therefore, this chapter describes the process steps for all variants together. The specific steps for a Basic, Extended, and Full TIR are described in separate chapters, since the differences are more pronounced here.

The general steps are the following:

- Step 1: Module selection
- Step 2: Scoping
- Step 3: Procurement
- Step 4: Launch meeting
- Step 5: Business overview workshop
- Step 6: Draft report and feedback
- Step 7: Finalisation of the TI report
- Step 8: Involvement of the RTP
- Step 9: Delivery of the TIR and completion of the TI phase



Step 1: Module selection

As explained in Chapter 4.5, the first step in any ART TI process is determining which TI module best fits the institution. This decision follows from a discussion between the TCT and CTL but is ultimately the responsibility of the CTL.

Milestone(s)

Description	Responsible
Agreement on the TI module and the selected variant for the specific ART test	CT

Step 2: Scoping

Once all the modules for the testing phase (threat intelligence/red teaming/purple teaming/gold teaming) have been selected, the institution can start the scoping process. This process is important for the TI phase, because in this phase the institution's CIFs, services and underlying processes are identified. 'Flags' to be captured can be placed on these key systems and services. The SSD is a key pillar that supports the TI report and should be approved during the scoping meeting.

Milestone(s)

Description	Responsible
Delivery of the SSD	CT
SSD approved by C-level sponsor and TCT	TCT, C-level sponsor

Step 3: Procurement

When opting for an external TIP:
In the procurement phase, the CTL reaches out to one or more TIPs to request quotations for the selected TI variant. The CTL clearly describes the expectations regarding the TI phase. The TI report requirements (outlined in Chapter 6 of this guide) are also shared in the request, making it more likely that the proposals received will match the institution's needs.

When opting for an internal TIP:
When the CTL decides to have the TI report prepared by an internal TI resource, external procurement is not required. Instead, the CTL must identify internal staff who meet the requirements outlined in Chapter 6. Similar to the external TIP procurement process, the CTL must provide a clear description of expectations for the TI phase to ensure the selected internal resources can successfully deliver the report. Additionally, the CTL must take appropriate steps to guarantee that the internal TI resources are properly isolated from the rest of the financial institution. This is to ensure the secrecy of the test.

Milestone(s)

Description	Responsible
Signed contract with TIP (internal or external)	CTL

Back to overview threat intelligence steps

Step 4: Launch meeting

Once the procurement is finalised, it is time to plan a launch meeting. The launch meeting marks the official start of the testing phase and more specifically the start of the TI phase. In this meeting, various practical agreements are made regarding the frequency of meetings during the TI and RT phases, communication channels, documentation and responsibilities. After the launch meeting, the TCT, CT and (if applicable) TIP hold weekly meetings to discuss the progress of the TI phase. During the launch meeting the CTL, TCT, TIP, RTP, GTP and C-level sponsor are all present.

Note: If the CT or the TCT feels that there are too many practical arrangements to be made in the launch meeting, they may organise an informal pre-launch meeting. This is intended to prevent the C-level sponsor from being unnecessarily involved in too many peripheral matters that are not relevant to their role.

Milestone(s)

Description	Responsible
Launch meeting held between CT, TCT, TIP and RTP	CTL, TCT, TIP, RTP, GTP and C-level sponsor
Agreement on the communication channels and setting up the schedule of meetings during the ART test	CTL

Step 5: Business overview workshop

This step is not mandatory but highly recommended during the TI phase of an ART test. Knowing the business processes, systems and their criticality is a vital part of writing a comprehensive TIR. Gaining this knowledge within the limited timeframe of the TI phase is challenging. Modern institutions are often highly specialised, making it challenging for external providers to fully understand business operations and client bases. To address this, the CTL can optionally organise a business overview workshop between the TIP and the institution's (senior) business expert. It is of the utmost importance that the TIP has a comprehensive understanding of both the technical components and the business processes of the financial institution. During this workshop, a business expert from the institution will help the TIP to get a better understanding of the CIFs and the underlying systems in the SSD. This will allow the TIP to more effectively assess the threats relevant to the institution. It is vital that the CTL makes sure that the business expert is (temporary) onboarded into the CT and, if deemed necessary, signs an NDA for the remainder of the test.

Milestone(s)

Description	Responsible
Organising and hosting a business overview workshop between an internal business expert and the TIP	CTL

Back to overview threat intelligence steps

Step 6: Draft report and feedback

During the TI phase, weekly update meetings are held to share the progress of the TI analysis. Based on that analysis, the TIP drafts the TIR, and shares it with the TCT and the CT. They give the TIP feedback on content and formal requirements, so the TIP can amend the report if necessary. There is no predefined moment in the TI phase when the draft version should be submitted to the CT and TCT, but the TIP should aim at a moment roughly halfway through the TI phase. The CTL keeps the C-level sponsor informed about the TI phase process and the early parts of the scenario, ensuring all stakeholders remain aligned with the direction of the TI phase.

The feedback from the CT and TCT covers the following:

1. Does the report meet the requirements outlined in Chapters 5.2 to 5.4?
2. Are the outcomes of the TI analysis presented in the draft TIR in line with the TCT's perspective on the cyber threat landscape? If not, does the TIP back up its alternative perspective with credible, publicly accessible sources?

Note: The TCT will provide only one set of comprehensive feedback on the draft TIR. The production and delivery of a TIR that meets all the ART criteria remains the responsibility of the TIP.

Milestone(s)

Description	Responsible
Producing and sharing the draft version of the TIR	TIP
Giving feedback on the draft version of the TIR	TCT and CT
Keeping the C-level sponsor in the loop on the direction of the TI phase	CTL

Step 7: Finalisation of the TI report

Based on the feedback provided, the TIP updates and finalises the TIR. Once again, it is important to keep all stakeholders informed on the progress of the TIR during the weekly updates to avoid 'surprises' when the final report is presented.

Milestone(s)

Description	Responsible
Finalising the TIR	TIP

Step 8: Involvement of the RTP (optional)

The CT can choose to involve the RTP at any moment during the TI phase. Although RTP involvement in the TI phase is not mandatory, it can facilitate a smooth transition between the TI and RT phases. A prime, timesaving example is that when the finalised version of the TIR is considered fit for approval, the CTL can share this version with the RTP. As a result, the RTP can already start drafting its RTTP before the TIR has been formally approved. This could save several weeks. However, the responsibility for the decision to use a version of the report that is not yet formally approved lies with the RTP.

Milestone(s)

Description	Responsible
Sharing the (draft of the) TIR with the RTP to support RTTP creation (optional).	CTL

Back to overview threat intelligence steps

Step 9: Completion of the TI phase

Once the feedback from the TCT and CT has been processed, the finalised document will be formally approved during the TIR go/no-go meeting. In this meeting, the TCT, CT (including the C-level sponsor), RTP and TIP discuss the final TIR. This includes a discussion on the scenarios that are to be selected for execution. If all parties agree on the quality, the content and – most importantly – the scenarios, the C-level sponsor gives a 'go' on the TI-led scenarios and the test can now progress to the next stage: producing the RTTP.

As mentioned in step 8, the TIR can be shared with the RTP before formal approval to speed up the process of creating an RTTP. This can only be done if the finalised TIR is deemed fit for approval by the reviewers. Formal approval of the TIR by the CT/C-level sponsor and the TCT marks the start of the red teaming phase of the test. This approval needs to be documented in writing. The final, approved TIR is shared with the RTP after the go/no-go meeting. The TI-based scenarios then serve as the foundation for the RTTP.

Milestone(s)

Description	Responsible
Organising and hosting a go/no-go meeting for the approval of the final version of the TIR.	CTL
Handing over the final, approved TIR to the RTP.	TIP
Approval in the form of a written statement.	CT/C-level sponsor and TCT

Back to overview threat intelligence steps

5.2 Specific requirements for Basic, Extended and Full TIR

This Chapter set out the specific requirements for the three TI variants. Please note: (1) These requirements refer to the TIR and not to the TIP. For requirements on the TIP please see Chapter 6. (2) These requirements serve as a minimum indication of what a report should include. The TIP may, with proper justification and in consultation with the TCT and CTL, deviate from these requirements. The following chapters are intended primarily as indicative guidance.

	Basic TI	Extended TI	Full TI
Document length	5-10 pages.	10-20 pages.	Minimum of 20 pages.
Executive summary	Included.	Included.	Included.
Business overview	General description of company activities and their critical functions.	Description of company activities and their critical functions + limited analysis of relation to threat actors and threat landscape.	Detailed description of company activities and their critical functions + thorough analysis of relation to threat actors and threat landscape.
Analysis of the SSD	A brief summary of the key critical functions as outlined in the SSD, along with the implications for the institution if these CIFs are impacted.	A more in-depth analysis of the critical functions as outlined in the SSD, along with the implications for the institution if these CIFs are impacted, using the CIA triad.	A comprehensive analysis of all critical functions as outlined in the SSD, along with the implications for the institution if these CIFs are impacted, using the CIA triad.
Analysis of the threat landscape	Basic analysis primarily based on the information from the GTL.	Detailed analysis tailored to the institution that gives a clear picture of the implications of the landscape for the institution. Sources include the GTL and the TIP's own TI platforms and information.	Extensive analysis of the threat landscape with a strong focus/analysis on implications for the institution. The TIP's own TI platform and intelligence position are the primary data sources for this variant.
Actors	A limited amount of +/- 3 threat actors.	A limited amount of +/- 5 threat actors.	A shortlist of +/- 5 threat actors that is derived from a longlist of at least 10 threat actors.
Scenarios	There should be two TI scenarios for every scenario executed in the RT phase. These scenarios should include a narrative, in, through and out, but with limited detail.	Two or more detailed scenarios for every scenario executed in the RT phase. These TI scenarios should include a more detailed in, through and out than Basic TI, but technical information on the threat actor is not mandatory.	A comprehensive list of scenarios from which a selection will be made for detailed elaboration. The selected scenarios will include an in-depth narrative, and in, through and out phases enriched with technical information about the threat actor.
Attack surface analysis	Not mandatory.	Not mandatory, but recommended.	Mandatory: technical information on both the chosen threat actors and the attack surface of the institution.

6 Overview of the provider requirements

This section gives an overview of the set of requirements for every type of TIP that can be selected for an ART test.

6.1 Introduction and overview

One of the core principles of ART is flexibility. This does not only apply to selecting modules and variants, but also to who is to execute them. The TI module is a prime example of this. Depending on the TI variant selected, different types of TIPs can be contracted. The following chapter first explains which types of TIPs are permitted to execute which TI variant. Subsequently, the requirements are presented. These are organised by TI variant rather than by provider type.

The table below indicates which type of TIP is permitted to execute each TI variant, including the likelihood of the given combination.

Most likely real-life application of the TI variants

	Internal resource	RTP	TIP
Basic TI	most realistic option, pending capabilities	most realistic option, pending capabilities	allowed, but not likely in practice
Extended TI	allowed, pending capabilities	most realistic option, pending capabilities	allowed, but not likely in practice
Full TI	not allowed	allowed, pending capabilities	most realistic option, pending capabilities

More information on this table will be provided in the following sections. Sections 6.3, 6.4, and 6.5 present a global overview of the TI requirements for the different variants. Additional information can be found in the ART Service Procurement guide.

6.2 Different types of TI providers

Internal threat intelligence capacity

Financial institutions' internal TI capacity may vary. For smaller institutions, this is typically very limited. Larger institutions on the other hand, often have teams of multiple experts working full-time to monitor the institution's threat landscape. Within ART, it is permitted to leverage internal capacity, if available, when executing the TI module. This depends on both the size and quality of the team and the complexity of the selected TI variant. The more professional the institution's internal TI capacity, the greater the likelihood that it will be authorised to execute the TI module.

Pros

+ No procurement process means shorter timelines
+ Cost-efficient
+ Internal TI experts know their own organisation best

Cons

– No fresh outside-in perspective
– More difficult to steer clear of internal politics
– More difficult to keep the ART test confidential if internal TI staff are involved
– The TI module should only be executed by internal staff who are up to the task

Red team provider with threat intelligence capacity

Financial institutions often consider it beneficial when an ART test requires only one procurement process. This is possible when the RT provider is also capable of delivering the TI capacity. Several RTPs have, to varying degrees, the capacity to produce in-house TIRs. For ART, this can be an attractive option, as mature RTPs are able to offer a range of TI variants. While a specialised TIP will generally not invest effort in executing basic TI, an RTP may often include this as an add-on in their RT proposal. A RTP can therefore offer the best of both worlds for a TI module, combining its TI capabilities with its RT expertise. When executing a TI variant, the RTP should be able to guarantee that its RT and TI functions are separated by Chinese walls in order to prevent cross-contamination.

Pros

+ Single procurement process
+ Relatively cost-efficient
+ Fresh outside-in perspective
+ Combining RT with TI knowledge
+ Not hindered by internal politics or legacy
+ The TIR can integrate seamlessly with the RTTP thanks to aligned formats, templates, and procedure

Cons

– Possible contamination between TI and RT functions
– TI can be written to fit the capabilities of the RT
– A good RTP is not automatically also a good TIP. Extra vetting of their TI capabilities might be required.

Specialised threat intelligence provider

This option closely resembles the TI phase in TLPT/TIBER, where a specialised TIP usually performs the TI of the test. In practice, specialised TIPs are generally most effective at conducting in-depth research on clients and their associated threats. These providers typically employ staff with expertise in identifying and analysing threat-related vulnerabilities and in reporting these findings in a structured and comprehensive manner.
The outcome is usually a high-quality (and high-volume) TIR containing potentially significant operational information that can directly enhance the RTTP.

Pros

+ This type of provider will generally provide you with the most detailed report
+ High degree of expertise
+ Fresh outside-in look
+ Not hindered by internal policies or legacy

Cons

– Usually the most resource-intensive and costly option
– The institution has to deal with a dual procurement process
– Generally only effective for the full TI variant

6.3 Requirements for the Basic TI variant

A basic TIR may be produced by internal TI capacity, an RT provider, or a specialised TI provider. Regardless of who executes this variant, the following requirements must be met:

- At least one dedicated individual should be responsible for the entirety of the TI process. More than one individual is recommended.
- The individual should work at a TIP or in a TI-related department.
- The individual has produced at least two TIRs/TI analyses over the last 24 months.
- The individual has an educational background in the field of TI.
- The individual has TI certifications as listed in the ART Service Procurement Guidelines.
- The individual has at least three years of experience within the financial institution or a similar institution.
- The individual has several years of hands-on experience with TI and has demonstrated working experience or professional interest in the field of TI in the financial services sector.

For the basic TI variant, the selected external/internal provider should meet **at least four of the seven** requirements, with the first requirement being mandatory. The more the better. In case of doubt, the TCT and CTL must discuss the suitability of the TI provider.

6.4 Requirements for the Extended TI variant

An extended TIR may be produced by internal TI capacity, an RT-provider, or a specialised TIP. Regardless of who executes this variant, the following requirements must be met:

- At least two dedicated individuals are responsible for the entirety of the TI process.
- The individuals work at a TIP or in a TI-related department.
- The individuals have produced at least two TIRs/TI analyses over the last 24 months.
- The individuals have an educational background in the field of threat intelligence.
- The individuals have TI certifications as listed in the ART Service Procurement Guidelines.
- The individuals have worked at least three years at the financial institution or a similar institution.
- The individuals have several years' hands-on experience with TI and have demonstrated working experience or professional interest in the field of TI in the financial services sector.

For the extended TI variant, the selected external/internal provider should meet **at least five of the seven** requirements, with the first requirement being mandatory. The more the better. In case of doubt, the TCT and must CTL discuss the suitability of the TI provider.

6.5 Requirements for the full TI variant

A full TIR may be produced by a RTP or a specialised TIP. Regardless of who executes this variant, the following requirements must be met. These are in line with the ART Service Procurement Guidelines for TI providers. Since this is the only variant with mandatory targeted threat intelligence, the requirements differ significantly from the other two variants.

Requirements at company level

- At least three references from previous assignments related to threat intelligence-led red team tests.
- Adequate indemnity insurance in place to cover activities which were not agreed on in the contract as well as those resulting from misconduct, negligence, etc.

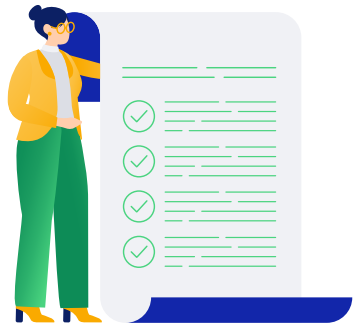
Requirements for TI Manager

- The Threat Intelligence Manager from the TIP is responsible for leading and overseeing the TI provider's activities when executing an ART test.
- The Threat Intelligence Manager from the TIP must have adequate experience in threat intelligence. Expectations: at least five years of experience in threat intelligence, including three years of producing threat intelligence in the financial services industry.
- The Threat Intelligence Manager from the TIP must provide an up-to-date CV and at least three references from previous assignments, specifically related to delivering threat intelligence for red team testing activities, to the institution.
- Background checks on the Threat Intelligence Manager are conducted by the TI provider (as a minimum). Enhanced background checks are conducted as required by the national authorities.
- Ideally, the Threat Intelligence Manager from the TIP holds relevant, recognised qualifications and certifications in threat intelligence.

Requirements for TI team

- The Threat Intelligence Team members must have adequate experience. Expectations for each member: at least two years of experience in threat intelligence.
- An up-to-date CV for each member of the team must be provided to the institution.
- The Threat Intelligence Team must have a multi-disciplinary composition, representing a broad range of skills including OSINT, HUMINT and geopolitical knowledge.
- Background checks on each member of the Threat Intelligence Team are conducted by the TI provider (as a minimum). Enhanced background checks are conducted as required by the national authorities.
- Ideally, the Threat Intelligence Team members hold relevant, recognised qualifications and certifications in threat intelligence.
- Ideally, the Threat Intelligence Team members have experience in delivering threat intelligence for red team tests.

For a more comprehensive explanation of the TI requirements for this variant, please see the ART Service Provider Procurement Guidelines.



Annex: List of abbreviations

ART	advanced red teaming
BOD	board of directors, also referred to as executive board
BT	blue team
CIFs	critical or important functions
CMT	crisis management team
CT	control team
CTL	control team lead
GT	gold teaming
GTL	generic threat landscape
GTP	gold team provider
GTTP	gold team test plan
LPT	limited purple teaming
NDA	non-disclosure agreement
OSINT	open source intelligence
PT	purple teaming
RFP	request for proposal
RT	red teaming
RTP	red team provider
RTTP	red team test plan
RTTR	red team test report
SME	subject matter expert
SOC	security operations centre
SSD	scope specification document
TCT	test cyber team
TI	threat intelligence
TIBER	threat intelligence based ethical red teaming
TIP	threat intelligence provider
TIR	threat intelligence report
TM	test manager
TPSP	third party service provider
TTP	tactics, techniques and procedures

De Nederlandsche Bank N.V.
PO Box 98, 1000 AB Amsterdam
+31 (0) 20 524 91 11
dnb.nl/en

Follow us on:
Instagram
LinkedIn
X

DeNederlandscheBank

EUROSYSTEEM