ART Control Team Guide

for the financial sector

DeNederlandscheBank

EUROSYSTEEM

Contents

1 About this guide

2 Requirements for setting up the control team

3 Roles, skills and responsibilities

4 Other considerations

Annex

1 About this guide

This document provides an overview of the requirements for setting up a control team (CT) and the roles, skills and responsibilities of the individual CT members. It also describes considerations that the Control Team Lead (CTL) and the CT must consider when preparing and managing an ART test. For a list of abbreviations, please refer to Annex A.

1.1 Purpose of this guide

The purpose of this guide is to provide guidance on how to set up and effectively run a control team (CT) in an ART-test. It covers the minimum requirements for setting up a CT, the roles and responsibilities of the CT members and the skills and experience of the CT members. It also covers the CT governance and an overview of the deliverables and milestones the CT needs to manage.

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:

- The control team lead (CTL)
- Members of the control team (CT) at the institution conducting the ART test
- The threat intelligence provider (TIP)
- The red team provider (RTP)
- The gold team provider (GTP)
- Test Cyber Teams (TCTs) or authorities involved in the ART test

1.3 Legal and disclaimer

This guide is intended for institutions that plan to use the ART framework for conducting 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, minimal requirements and attestation

When an institution intends to conduct an ART test, the ART framework and its underlying guides provide the minimal requirements that should be met when conducting the test. To make sure the quality of the test meets the ART standards, the lead test manager (TM) from the DNB Test Cyber Team (TCT-DNB) will be present. The TM will be present in all phases of the ART test to ensure the test is prepared, conducted and evaluated following the requirements as presented in the ART framework and its underlying guides.

At critical moments in the test, TCT-DNB provides an approval on certain deliverables, such as the SSD, the TIR or the RTTP. This will always happen in close collaboration with the CT and TIP, RTP and/or GTP. Next to the quality assurance (QA) role, the TM is a sparring and guiding partner for the CTL who holds the ultimate responsibility for the ART test within the institution. If the test has been conducted in accordance with the requirements of the ART framework, TCT-DNB will provide the institution with an attestation document concluding the test.

2 Requirements for setting up the control team

2.1 Purpose of the control team

The CT is the body responsible for the end-to-end conduct of an ART test and managing the separate phases of the test. The CT members are the only staff within the institution that are fully aware of the test. Since the test activities are conducted on the institution's production systems, it is essential to minimise the risk of disrupting the institution's daily operations. Therefore, a major objective of the CT is to ensure that the test is conducted in a safe and controlled manner by identifying and managing risks throughout the process. The CT also acts as the main link between all the internal and external parties and stakeholders involved in the test.

2.2 Composition of a control team

The composition of the CT depends on several characteristics, such as the size, the organisational structure and the business model of the institution. This means the composition of the CT may vary from institution to institution. However, the guiding principle is that the CT should be as small as possible to maintain secrecy of the test. It should only include those people with the appropriate skills and knowledge of the institution to manage the test end-to-end.

The CT's composition needs to be balanced to ensure it has sufficient business and operational knowledge of the institution and its critical or important functions (CIFs), systems and processes, and has the right level of authority or mandate to make critical decisions during the test. Depending on the test phase, roles can be added or adjusted to ensure the necessary knowledge and expertise are available to manage the test effectively at that stage.

The following roles are advised to be included in the CT:

- A CTL and one back up (mandatory)
- A C-level sponsor (mandatory) and preferably one back-up
- Subject matter experts (SMEs) such as an IT architect, a security architect, a risk manager and/or a procurement specialist (optional and maybe temporarily)
- A representative of each ICT third party service provider (TPSP) (optional)
- A member with threat intelligence (TI) expertise (optional, depending on the TI variant selected)
- A member with crisis management expertise, who is not partaking in the gold teaming (GT) exercise, having the role of GT lead (mandatory when a GT module is selected)
- Other experts, as required (optional).

2.3 Validation of the composition of a control team

No later than at the start of the test the institution selects a CTL. The CTL then selects the other members of the CT based on their expertise. It is the responsibility of the CTL to form an appropriate CT for that specific test.

The test manager (TM) must validate the final composition of the CT and any further changes to it. If there are any concerns about who is selected to be the CTL or to be a member of the CT, the TM has the authority to address this as an operational risk for the test and to encourage the CTL to manage that risk accordingly. Failure to address an operational risk may have consequences for the ART attestation (see Section 3.6 of the ART framework).

2.4 Stakeholders for the control team

The CT has a number of important stakeholders. Some of these stakeholders are aware of the test during all phases of the test. Some will only be aware of the test when the test is detected or when a specific module of the test is executed, such as GT. The most important stakeholders are:

- The institution's board of directors (BOD)
- The RTP
- The TCT and the test manager (TM)
- The TIP (optional)
- The GTP (optional)
- The institution's crisis management team (CMT) (optional)
- The institution's blue team (BT) (optional)

Depending on the modules selected for the test, the number of stakeholders may vary. The BT or the members of the CMT – when GT is selected – should not be made aware of the test before the completion of the active red teaming (RT) or the execution of the GT module. However, when the BT detects any test activities (or parts of the test) before the test has been completed, (a representative of) the BT might be included in the CT. Until that moment, they should be an (unaware) stakeholder of the CT.

Also the role of possible TPSPs should be taken into account. Please refer to paragraph 3.4 for guidance on the incorporation of these TPSPs in the CT or should be seen as an external stakeholder.

2.5 Responsibilities of the control team

The main responsibilities of the CT are:

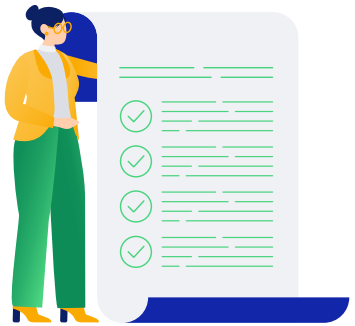
- Ensuring that the execution of the test is in compliance with the requirements as outlined in the ART framework
- Providing (informational) leg-ups, and to do so in good time in order to maximise the learning experience of the exercise
- Informing the involved management of the institution about the progress of the test and the associated risks
- Ensuring that all risk management controls are in place and operating effectively, so that the test can be conducted in a controlled manner
- Ensuring that any business impact from the test is within the institution's risk appetite
- Ensuring that the institution's relevant CIFs are included in the scope specification document to facilitate a realistic simulation of an actual advanced targeted attack
- Facilitating the procurement process of the provider(s) in accordance with the ART service provider procurement guide
- Liaising closely with the provider(s) and the TMs throughout the test, using the agreed communication channels
- Ensuring adequate insights in and manage any potential escalations arising during the test
- Taking informed decisions throughout the test
- Maximising the learning experience for the tested institution
- Consulting with the C-level sponsor in the CT to ensure that the relevant deliverables are signed off in accordance with the ART framework.

The roles, skills and responsibilities of the individual (mandatory and optional) members are outlined in Chapter 3.

2.6 Control team governance

The ART test is performed under the responsibility of the tested institution. The institution's board of directors should delegate the responsibility for the end-to-end and day-to-day management of the test to the CTL.

The CT must operate separately and independently from the internal or external TIP, RTP, GTP and BT. Because of the responsibilities mandated to the CT, they can make decisions that have a significant impact on the test, and potentially on the continuity of the institution's CIFs. Therefore, the institution must ensure that the governance arrangements regarding the CT are well-considered and robust. It should be noted that the ultimate accountability for the test and its outcomes always remains with the board of directors of the institution.



3 Roles, skills and responsibilities of the individual CT members

This chapter describes the roles and responsibilities of the CT members and how they interact with the relevant stakeholders. CT members must have the necessary skills and experience/ expertise to ensure they are able to fulfil their roles in the CT.

3.1 Control team lead (CTL)

3.1.1 Role description

The CTL is responsible for selecting the CT members, for the day-to-day management of the test, the decisions to be taken and the documents to be delivered. The CTL is the primary point of contact for the CT members, the CT stakeholders and the TM.

The CTL must have the authority, mandate and time to take full control of the test process and must have direct access to senior management and/or other relevant individuals that are important for the test.

The CTL will need at least 8-12 hours per week on average to prepare and complete the necessary documentation, decisions and meetings. Throughout the entire test period, they will also need time to prepare the necessary information and/or leg-ups to meet deadlines and to maximise the learning effect of the test.

Due to the importance of this role, it is essential to also have one backup CTL, who has access to the same information about the test details as the primary CTL. This is to ensure that the management of the test can be continued if and when needed.

3.1.2 Skills

The CTL requires skills in several different fields of expertise, since they bear ultimate responsibility for the overall test and are the primary point of contact for all stakeholders. The CTL benefits from having knowledge about the institution's (cyber) security posture and having a close relation to the institution's security operations. The skillset a CTL should possess consists of:

- Strong project management skills such as planning, management of deliverables and milestones, risk management and resource management
- People and process management skills
- Ability to communicate with different levels of staff, from C-level to operational teams and departments including legal, procurement, IT security and business areas
- Ability to work under pressure
- Ability to be pragmatic and decisive, such as by providing guidance and clarity in case of an escalation.

3.1.3 Experience

In addition to the skills listed above, a CTL should also have expertise in additional areas. If the CTL lacks this experience, other members in the CT should be able to supplement it. Ideally, the CTL should have the following experience:

- A thorough understanding of the institution's core processes and its supporting IT landscape and business operations
- Experience in leading cyber resilience exercises, specifically red team testing
- Experience in managing escalations related to cyber or IT incidents and crisis management
- General knowledge of privacy and security and specifically their legal aspects, including the ability to identify when it is necessary to involve the legal department
- Experience with procurement processes including knowledge of the relevant vendor market.

3.1.4 Responsibilities

The institution's board of directors should delegate the responsibility for the management of the test to the CTL. The CTL therefore has a delegated responsibility for:

- The day-to-day planning and management of the end-to-end test process consisting of all selected modules, including the timely delivery of all mandatory deliverables and reaching all mandatory decisions and milestones according to the ART framework[1]
- The assessment and follow up of the outcomes of the risk management process during the end-to-end test execution
- The preparation and signing of the contract between the TCT and the authorised person within the institution as a prerequisite for the ART exercise to commence
- The timely procurement of TI, RT and (if applicable) GT providers
- The decision on which modules of the ART framework the institution wants to include in the test
- The composition of the CT
- The management and record keeping of all decisions made during the test
- The cleaning up of all traces of the test from the IT systems and the restoring of the pre-test situation, when and where the RT is unable to do so.

3.1.5 External resourcing of the control team lead

As long as the responsibilities and tasks for the CTL are managed, this role could also be delegated to an external resource. However, the institution itself is ultimately responsible and accountable for this external resource's compliance with the CTL-requirements and the responsibilities set out in the ART framework and this CT guide. If the external CTL does not have the required skills and experience, the other members in the CT should be able to supplement these. In addition, there should always be a backup CTL.

Given the intrusive and confidential nature of the test, the institution should take all the usual precautions like vetting, having the external CTL sign a non-disclosure agreement (NDA) and ensuring that no sensitive data is retained by this individual and the company for which they are working.

If the external CTL is resourced from a specialist external provider, the institution should carry out the required due diligence research on this individual and the provider. This is to ensure that the CTL has the right skills, experience, qualifications and security measures in place to manage an ART test.

To avoid any conflict of interests, the external CTL cannot also work for the TIP, RTP or GTP that is procured for executing the TI and/or RT and/or GT activities for that test. All these arrangements should be formalised in a contract.

3.2 C-level sponsor and its tasks and responsibilities

The C-level sponsor of the CT should be a member of the institution's board of directors. This could be the COO, CIO, CTO or equivalent, as long as it is the most senior individual on the CT to be able to act as the escalation point during the test. When critical decisions need to be made on how to proceed with the test from the institution's risk management perspective, the CT needs to have adequate seniority to be part of the decision-making.

Although the C-level sponsor is unlikely to be the CTL or have an active and resource-intensive role during every step of the test, their (ad-hoc) presence on the CT will allow the CTL to escalate matters in full confidentiality.

1 The ART quality assurance format is provided to support the CTL in managing these process steps, deliverables, milestones and decisions.

Furthermore, the C-level sponsor in the CT is responsible for the formal approval of all deliverables, such as the scope specification document. The C-level sponsor (and the optional back-up) is also responsible for ensuring awareness and management of the risks and benefits of the test at board level, both during and after the test.

If the gold team module is included in the test, the C-level sponsor to join the CT cannot also be part of the crisis management team (CMT). This is because the executed GT scenario must remain confidential for the CMT participants for the sake of realism and for maximising the learning experience on this part of the test. When the responsibility for crisis management exercises is mandated to another member of the board than the responsible board member for IT security matters, it should be clear which board member(s) will take on what responsibility.

There are no additional skills or experience requirements for the C-level sponsor in the CT, as the requirements for C-level functions are predefined by the institution.

3.3 Subject matter experts and their tasks and responsibilities

Subject matter experts (SME) can be included to enable the CT to prepare and develop the required deliverables with as much knowledge of the institution as is needed. This might be the case for drafting the request for proposal for the TI and/or RT providers, the scope specification document, when additional information is needed during the active red team phase or on any other occasion during the process. CT members that can be added as SMEs could include an IT architect, a security architect or a procurement specialist.

Adding these SMEs will allow the CTL to make the appropriate risk-based decisions during the test. The number of SMEs to be included in the CT will vary from institution to institution. SMEs with the broadest range of knowledge should be selected where possible, to minimise the number of people having knowledge about the test and maximise the chance of remaining the secrecy of the test.

SMEs could have the following specific skills and experience:

- Extensive and specific knowledge of the business processes within the institution
- Extensive knowledge of the field of expertise in which they are the SME
- Extensive knowledge of the IT landscape, including the security setup of the institution
- Sufficient risk management knowledge
- Sufficient experience in project management
- Experience in cyber resilience testing, including red team testing
- Sufficient and up-to-date knowledge of tactics, techniques and procedures used by cyber threat actors.

Not every SME needs to possess all of the above-mentioned skills and experience, but all skills and experience should be covered by the CT as a whole.

3.4 ICT third party service provider representatives and their responsibilities

If the institution outsources the provision of (part of) their CIFs or other parts of their IT infrastructure to one or more TPSPs, representatives of the TPSP can be included in the CT. It is advisable for the CTL to have an early discussion with a trusted contact from the TPSP(s) on the need and options for inclusion. This could be done after a discussion with the TM in the early stages of the test, for example when drafting the scope specification document and when discussing the added value of including the TPSP(s) in the test.

Besides contractual obligations, representatives of TPSPs in the CT should be a trusted supporter of the ART concept and have an institutional mandate for this role.

TPSP representatives may add the following skills to the CT:

- Extensive and specific knowledge of the business processes and systems they provide to the institution
- Extensive knowledge of the field of expertise in which they are the subject matter expert
- Extensive knowledge of the IT landscape, including the security setup of the TPSP organisation
- Sufficient risk management knowledge.

In any case, the potential participation of a TPSP in the test and in the CT should be confidentially discussed with senior management at the TPSP. This is to ensure that the integrity and confidentiality of the test are maintained, also given the fact that TPSP staff members might be part of the BT.

The TPSP is subject to the same confidentiality requirements as the institution. Therefore, only a limited number of TPSP staff should join the CT, depending on the defined scope of the test. These staff members should have detailed knowledge about the systems provided by their organisation that the institution uses. Regardless of the involvement of TPSPs in the CT, the institution being tested remains ultimately responsible and accountable for the test.

3.5 Internal TI resources and their tasks and responsibilities

If internal TI resources are used to perform the threat intelligence analysis and reporting, a representative of these resources should be included in the CT. This is only the case if those TI variants are selected where the internal TI resources are responsible for these tasks.

The internal TI representative is responsible for:

- Communication and alignment of the TI milestones within the CT
- Delivery of the TI deliverables of the test.

Please refer to the TI guide for guidance on how to select the appropriate TI variant and the requirements for using internal TI resources.

3.6 Crisis management experts and their tasks and responsibilities

If the optional GT module for a crisis management exercise is selected in one of the three gold teaming variants, a member with crisis management expertise – the GT lead – should be added to the CT. The planning and preparation activities of the GT module are strongly connected to the TI and RT and could run in parallel with the execution of the TI and RT phases. Therefore, this GT lead should be included in the CT from the start of the test.

It is of utmost importance for maximising the learning objectives of the GT exercise that the crisis management expert in the CT is not one of the resources partaking in the GT exercise itself, nor should be a member of the institution's CMT. Only by maintaining the secrecy of the variant, scenario and timing of the GT, the reality and learnings of the GT exercise can be maximised.

The representative having the crisis management expertise is the GT lead within the CT and is responsible for:

- Drafting the high-level objectives and learning goals of the GT exercise
- Providing input for the procurement activities for the external GTP
- Providing input for and/or drafting the GT plan and assuring the connection and alignment between the RT phase and the GT exercise
- Aligning the planning of the GT exercise with the overall CMT agenda of the institution.

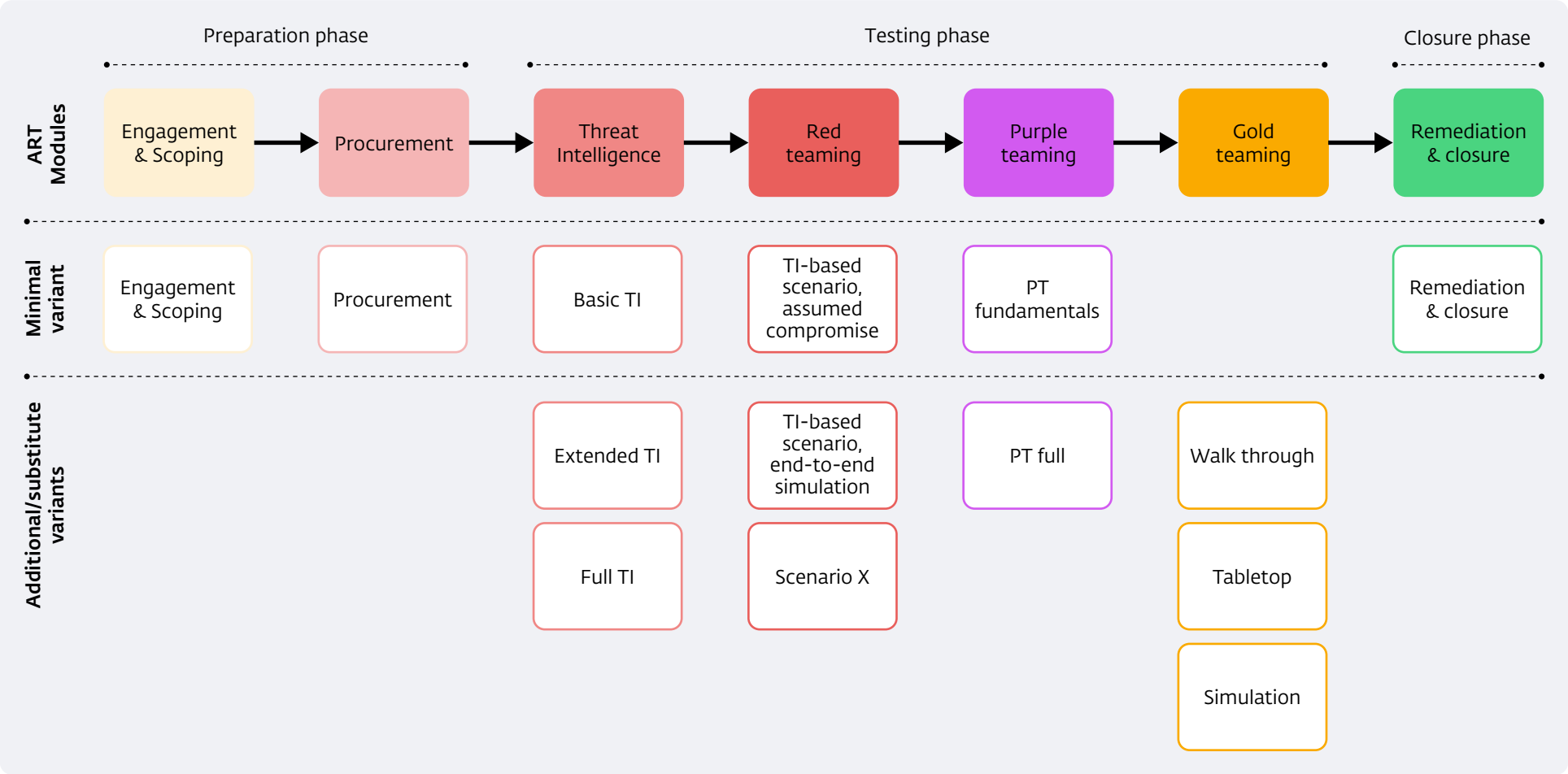
The CT lead could also take on the role of the GT lead, as long as this person has commitment from the crisis management portfolio holder in the board and has the required skills and expertise. If this is the case, it could be

considered to have the CTL – also performing as the GT lead – as the (single) CT member to hold the GT knowledge and responsibilities.

For further guidance on the role, deliverables and variants of the GT module, please refer to the GT guide.

3.7 Other optional experts and their responsibilities

During different phases of the test, specific expertise might be needed (such as procurement, legal or HR expertise). While these SMEs will not be included as day-to-day members of the CT, they should be informed about the high-level process of the ART test and the need for secrecy. These SMEs may be requested to sign an NDA to ensure the confidentiality of the test.



4 Other considerations

4.1 Role of the test manager and interaction with the CT

The TM is not part of the CT but works closely together with the CT during the entire test. As the TM is the main contact at the TCT for the CT, the TM should be consulted on all important issues throughout the test. The guidance given by the TM is one of the crucial operational controls in performing the ART test and helps ensuring a uniform, high-quality test containing all the mandatory elements.

To facilitate open communication and a successful learning test, it is critical that the CT and TM take a collaborative approach and foster a spirit of trust and cooperation. Clear communication channels between the CT and TM are paramount. The TM and the CT should regularly discuss if the test still meets the ART framework requirements to ensure that the learning experience of the institution is maximised.

4.2 Contractual agreements regarding the ART modules

Before the formal start of the ART test, the CTL and TM hold several initiation meetings to determine which ART modules best fit the institution's desired learning experience. The results of these discussions are formalised in contractual agreements between the institution and the TCT during the engagement steps.

Once agreed, the TCT will invoice the institution for test guidance costs. These costs are based on the modules and variants selected for that specific test by the institution.

4.3 Time resources

During all the phases of the test, the members of the CT must be able to dedicate enough time to their respective roles. On average, the role of the CTL takes approximately 8-12 hours a week for the total duration of the test. The other roles in the CT will, on average, take at least 4 hours a week from the moment they are included in the CT until the end of the test. This depends on the modules selected, the complexity of the institution and their CIFs, the duration of the testing phase and the experience levels of the different people involved.

4.4 Risk Management

During the preparation of the ART test and throughout the whole exercise, the CT should have a strong focus on identifying, classifying and managing the risks related to the test. These risks should be documented in a risk register, and the CTL should be in full control of the management of these risks. The identified risks and the actions to be taken to mitigate these risks should be discussed during the regular meetings where the TM is present. The TM can then assess whether the CTL and CT are sufficiently in control of managing the risks that the test might bring forward.

When the TM finds that the CT is not in control of the risk management process, the TM may, as an ultimate measure, and after repeated requests to assume control, remove the ART label from the test. If the ART label is removed, the institution can continue the test for learning purposes but will not be issued an attestation document.

4.5 Managing escalations after detection

If actions taken by the RTP are detected during the red teaming phase, it is likely that the BT will escalate this detection, considering it to be a real cyber attack.

Escalation is a key part of the test, as the ART test aims to evaluate the institution's detection and response capabilities. However, just like all other parts of the test, it needs to be controlled. For this reason, it is important for the CT to manage the possible escalation paths within the institution. The CT should however only intervene and stop an escalation if it will have an unwanted business impact or will involve external parties where this is not feasible.

An example of an uncontrolled escalation could be the shutdown of business-critical IT infrastructure by the BT to stop the attack, and/or the filing of a police report. In such cases, the CTL could intervene and pause the test and deal with the escalation. This should be done in close communication with the CT, TCT and RTP. At the same time the CTL should try to disclose as little information as possible for the test to be continued in secrecy. In such cases, the intervention of the CTL to stop the escalation could go via the appointed C-level sponsor of the CT, depending on what is agreed between them.

4.6 Considering the 'out' actions

Once the test reaches the final steps of the 'through phase', careful consideration of the actions to be undertaken during the 'out phase' is required. Before the start of the out actions, the RTP, together with the CT and TM must determine if the out actions – as described in the RTTP – are still aligned with the current planned execution of the scenario. If that is not the case, the RTP must specify how it will approach the new out phase, bearing in mind that the approach is still in line with the treat actor and scenario.

The actions to be taken in the out phase always must be discussed with and agreed by the CT and the TM before they are executed. This does not have to be recorded in a formal document, but the CTL must have a record of the discussion and decisions taken in the discussion of the out actions.

4.7 Confidentiality and NDA

To maximise the learning experience of the ART test, no one outside of the CT should be informed about the test. If the BT is informed about the test, the integrity of the test will be compromised. In the case that the institution and/or the CT inappropriately discloses details of the test to the BT, the final attestation of the test may be withheld by the TM.

However, conducting such intrusive tests secretly without people outside of the CT becoming aware, can be difficult. Furthermore, it may prove to be problematic for the CT members to conduct their daily tasks and responsibilities without raising suspicion. In such cases, as a form of protection for the CT members and to ensure that confidentiality is kept, the CT members could sign a confidentiality or NDA at the inception of the ART test or get a letter of indemnity from their institution.

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