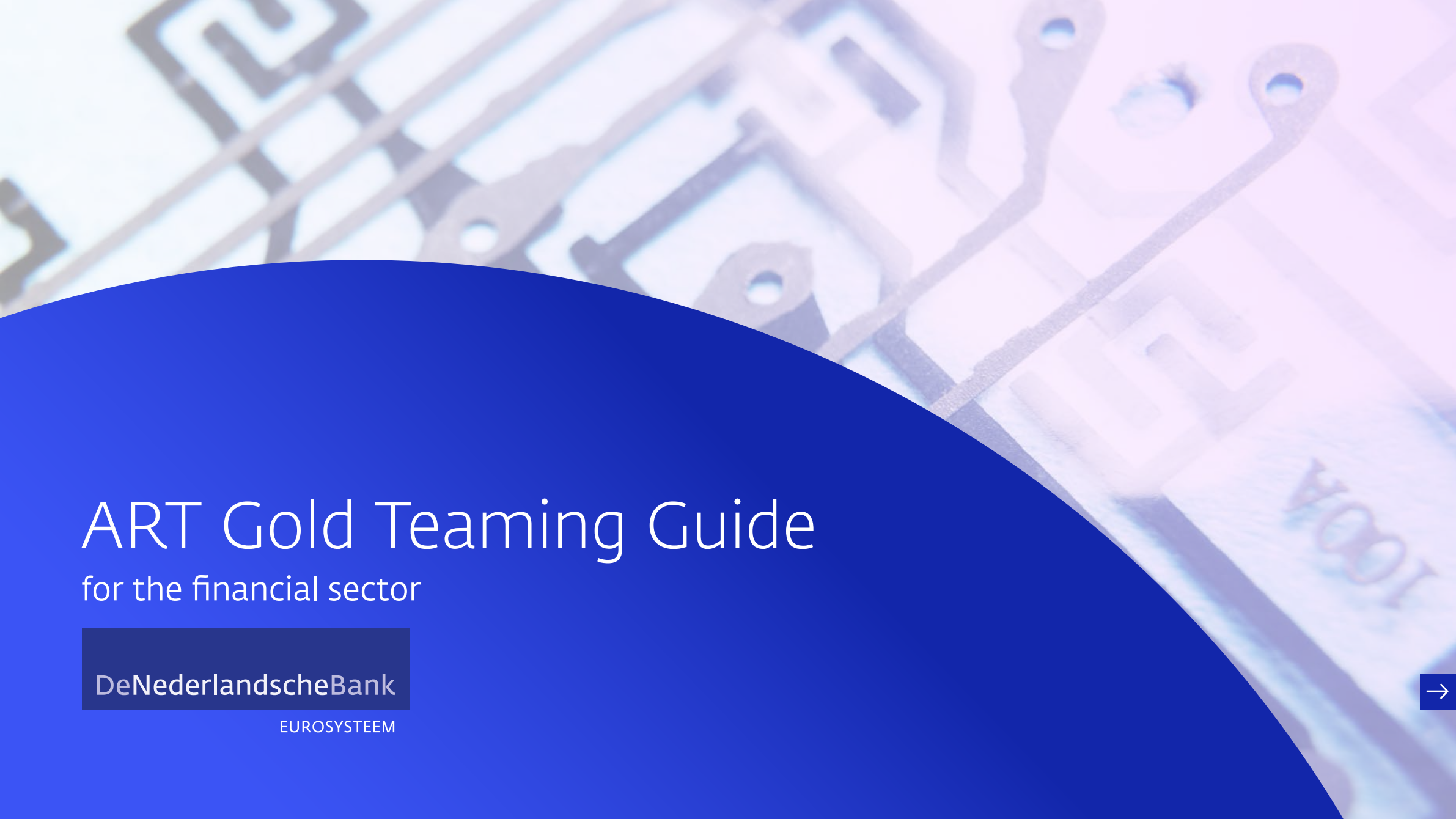


ART Gold Teaming Guide

for the financial sector

DeNederlandscheBank

EUROSYSTEEM

Contents

ART website & documentation

1 About this guide

This document first provides a short introduction to Gold Teaming (GT). This is followed by a description of the core principles of GT, highlighting the most important rules for GT and how it differs from traditional crisis management team (CMT) training and cyber exercise activities. After this, the different GT variants are described. Finally, the steps in planning, preparing, executing and evaluating a GT are described. For a list of abbreviations, please refer to annex A.

1.1 Purpose of this guide

This GT guide has been developed for the optional GT module in the Advanced Red Teaming (ART) framework as described in the framework in section 5.4. This guide offers guidance on the planning and preparation, execution and evaluation of a GT module in the scope of an ART test, and lays out minimum requirements, milestones and tips for GT.

1.2 Target audience

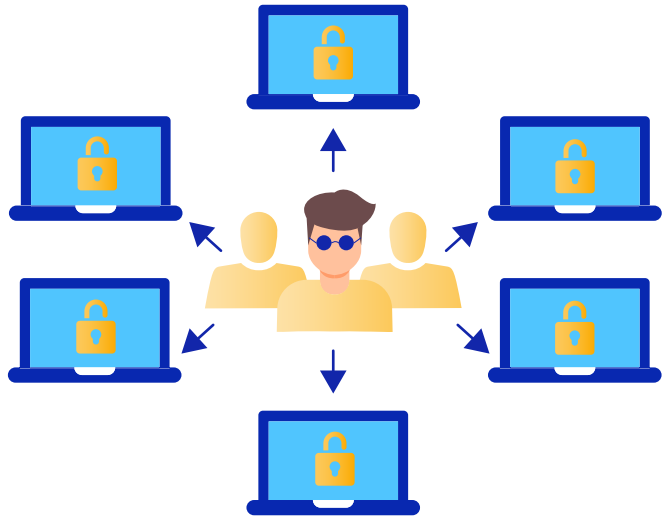
This document is intended for use by control teams (CTs) who are responsible for the ART test within the entity internal project teams and gold team providers (GTPs) to help them run a GT module.

1.2 Legal and disclaimer

This guide is intended for entities that plan to use the GT module in the scope of an ART test. Nothing in this guide should be construed as legal or professional advice. This guide is underlaying document of the ART-framework. For information on copyrights and creative commons, please refer to section 1.4 of the ART framework.

1.4 Role of the TCT, minimal requirements and attestation

When an entity chooses to include the GT module, this module is an integral part of the ART test. As a module in ART, GT is strongly connected to the threat intelligence (TI) and red teaming (RT) modules. To make sure the quality of the test meets the ART-standards the DNB Test Cyber Team (TCT) is present. The TCT will be present throughout the GT-module (and other modules) to ensure the GT 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 GT plan. This will always happen in close collaboration with the CT and GTP. Next to the quality assurance (QA) role, the TCT is a sparring and guiding partner for the CTL who holds the final responsibility for the ART-test within the entity, and the GT project team. If all requirements are met, the GT module will be signed off by the TCT in the attestation document during the closure phase of the test.



2 Introduction

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

2.1 What is the gold teaming module in ART?

The Australian CORIE Framework (Australian Council of Financial Regulators, 2020) first introduced the concept of gold teaming exercises in the field of ethical hacking and resilience testing for the financial sector. In ethical hack testing, the 'red team' refers to the attacking team and 'blue team' to the defending team. In ART, the 'gold team' refers to the team that holds ultimate responsibility for managing (cyber) crises at the strategic level: the CMT or board.

GT is a crisis management module that could be part of an ART test. For this module, the entity can choose from three different and increasingly complex variants: a walk-through session (WS), tabletop exercise (TTX) or simulation (SIM). For all variants, the scenario builds on the technical RT scenario and includes actual findings of the RT phase of the ART test. The DNB TCT facilitates and guides the institution's CT and GT project team (internal or external from a provider) through the framework.

2.2 What is the purpose of gold teaming in ART?

The RT phase of an ART test stops when the technical flags are achieved, or when the CT and TCT decide to end this phase of the test. However, there is a lot of potential for enhancing crisis management and organisational resilience in the period after the RT. The GT module has been introduced to harness that potential. This module can help tested entities benefit more from an ART test by getting the CMT involved, thus elevating the learning experience of an ART test to the strategic level.

Compared to traditional CMT training an exercising activities, a GT scenario within an ART test is TI and evidence-based (please read more on the TI and evidence-based nature of the GT scenario in section 3). This makes the GT module realistic in terms of the scenario that is used for the session. Because the scenario of the GT is based on the findings from the RT phase, the GT module makes the strategic implications of the technical findings accessible and more realistic to senior management. GT is therefore also an important tool to enhance cybersecurity awareness at the senior level.

2.3 What are the goals of gold teaming?

After the completion of the flags in the RT phase, a crisis management response by the tested entity would commence if the emulated technical scenario would have been a genuine cyber-attack. In the case of such an attack, effective crisis management by the entity's CMT is crucial to successfully mitigate the strategic impact of the attack. GT enables companies to benefit from this opportunity to practice such crisis response by integrating a CMT session in the ART test.

The primary goal of GT is to validate and test crisis management structures, plans and procedures, and to train and exercise managing the strategic impact, following a scenario as played out in the RT phase. A secondary goal is that GT makes the strategic implications, and required decision-making, of the test's technical findings accessible to senior management by incorporating these in CMT exercises. Third, successful GT can increase personnel's resilience, both during 'normal' day to day business operations and times of disruption and crises.

2.4 Who is gold teaming for?

A well-drafted and executed GT module in the scope of an ART test is a powerful tool for all entities, regardless their maturity level. The GT module is included in the ART framework for all entities that would like to enhance their crisis management capabilities, organisational and personnel's resilience.

Next to the organisation's maturity, practical boundaries such as available means, and specific learning goals are important variables in developing a GT module. A GT module is therefore always tailor-made to the organisation's needs and wishes.
To ensure a right fit for all entities that want to include a GT module in their test, ART offers three GT variants. For a detailed description on the GT variants please refer to section 4.

3 Core principles of gold teaming

In this chapter, the core principles of GT within an ART test are listed. These core principles give the reader an idea of which notions, ideas and concepts are central to designing the GT 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 selected variant, a GT module may involve elements of stress and rapid-fire decision-making, which can challenge your personnel's and team's resilience. To develop crisis management skills, a safe learning environment must be created and maintained throughout all steps of the module. Sufficient CT and TCT confidence in safety, capacity and expertise throughout the GT module is essential. When in doubt, the CT and the TCT can discuss how to enable this safe and capable learning environment.

- **GT is a strategic matter –** GT trains and exercises the crisis management function of the entity that is undergoing an ART test. Crisis management is inherently a strategic matter and should therefore at least involve the CMT of the tested entity. In the simulation variant (see section 4), tactical and/or operation teams such as (major) incident management teams and Computer Emergency Response Teams (CERTs) may also be involved to train and exercise cooperation between teams from different levels of the organisation.

- **Threat intelligence and evidence-based** – A GT scenario is always based on the scenario (or one of the scenarios) emulated in the RT phase of the ART test; the GT thus adds on to the technical findings from one of the RT scenarios, rather than combining findings from different scenarios. This means that the GT scenario is:

  - *Threat intelligence-based*, as the GT scenario builds on recent threat intelligence on advanced cyber threat actors from the TI and RT phase. Realistic threat actor details and behaviour must also be considered and included in the development of the additional, strategic crisis scenario for the GT. For example, in the case of a GT ransomware scenario: realistic ransom notes and the way the threat actor extorts in the organisation should be included.
  - *Evidence-based*, as the scenario is based on the technical RT findings and the actual impact those technical findings could have on the entity's operations, safety, security, finance and reputation if the test was an actual attack by a threat actor. The findings retrieved from the scenario (or one of the scenarios) in the RT phase should thus be used as input for the GT. If there were few findings in the RT phase, the GT is executed on the assumption that the flags from the RT phase were reached.

- **Alignment with the RT phase** – when selected as a module in an ART test, GT is an integral part of the ART test. It cannot be stressed enough: the GT scenario builds upon the RT phase and the (impact of) technical findings. Smooth cooperation and coordination between the red team provider (RTP), GTP (or internal project team) and CT is therefore crucial to a succesful GT assignment. To develop a realistic GT, it is important that the GT takes place shortly after the RT phase. This enhances the effectiveness of both phases. Senior management will feel less of a sense of urgency if the RT took place months ago and a full remediation programme has already started.

- **Executed by professionals with demonstrable experience** – developing, executing and evaluating a GT requires a combination of specific knowledge and skills. For that reason, it must be done by professionals. These professionals (both internal or external GTP) should have demonstrable experience and must be capable of working closely together with the RTP and internal organisation. You will find more specific requirements for staffing and procurement in sections 5.2.

- **Mandate** – C-level mandate (aware and agreed) is required before participating in an ART test. This goes both for testing on live production systems, as well for the planning and execution of a GT, as this can be a demanding exercise and it may therefore have a psychological impact on personnel. Also, findings and recommendations resulting from the GT might require C-level mandate to be mitigated or resolved.

- **Based on learning goals and sufficient planning –** the learning goals that are defined in the early planning stage of the GT run as a common thread throughout the GT assignment. Just as for the RT, the GT is deliberately planned: the more complex the GT variant, the more thorough the GT plan and planning. For example, if the SIM variant is selected and the exercise set-up contains an element of surprise (unannounced exercise) for participants, sufficient containment measures should be in place.

- **Confidentiality** – is of vital importance during all ART modules, also during GT. Planning and preparation activities of the GT module run parallel to the execution of the TI and RT phase, which are highly confidential. The ART-test may not become known within the organisation through a leak about a CMT session that is being prepared which follows upon a red teaming test. The code name of the ART-test also applies to the GT module. Depending on the learning goals and set-up, even the GT must remain confidential until the session is kicked off. Also, the GT-scenario must remain confidential for the CMT participants for the sake of realism.

4 Gold teaming variants

A CMT session based on a scenario that adds on the RT phase and scenario is a powerful tool. ART offers three increasingly complex GT variants to make it accessible and worth doing for all entities, regardless of their maturity level. This section details these three GT variants, each with its own set-up, investment and expertise. Please see the table in section 4.4 for an overview of the differences and similarities between the three variants.

4.1 Walk-through session (WS)

This GT variant is the most low-key and accessible GT variant. WS is a discussion-based session designed to validate the crisis management plans and processes and to increase the CMT's understanding of how to act in the event of a crisis. The WS is for entities with no or very limited experience in crisis management. The WS could also be the right fit for entities that have seen significant changes in their crisis management structure and personnel or are developing their crisis management function. The relative investment in a WS is (in most cases) the lowest of all variants in terms of resources and time. For this GT variant, a high-level scenario description is required plus a limited number of preparatory activities by the project team. It can therefore be a solution for organisations that want to validate their crisis management process with relatively few resources.

This variant does not contain elements of stress and urgency. During the session the participants (depending on learning goals) walk through all steps in the crisis management process as included in their plans, from detection to closure, in detail, based on a scenario that builds on the RT phase. Depending on the learning goals, a WS can also address roles and expectations between CMT members, and actions and measures to be taken in specific crisis scenarios ('what if' session). The WS is led by a facilitator/observer with in-depth crisis management expertise. The session should be observed to identify points and actions for improvement. The minimal duration of a WS is 2 hours.

4.2 Table-top exercise (TTX)

This variant is an accessible, discussion-based exercise and a good fit for entities with a CMT that already have some experience in crisis management, but who do not want to subject their CMT to a full simulation. The goal of a TTX is to train and practice crisis management in a low-stress environment. In this variant, participants receive scenario information step-by-step, which requires a storyline based on central dilemmas. Only limited elements of time pressure may be involved in the TTX. The investment for the TTX is in most cases higher than the WS. A more detailed storyline and detailed scenario information and events called 'injects' (such as phone calls, emails, messages on social media channels) should be developed and specific training and observational skills are required for evaluation purposes. TTX requires more staff-hours and additional skills than the WS variant, both during the preparation and the execution of the module.

The TTX variant enables CMT members to gain knowledge and skills on an individual level, but it also trains their ability to respond to challenges and work effectively as a team. During the TTX, participants are trained in specific crisis management capabilities, such as gaining situational awareness, communicating actions and statements, information management and decision-making (depending on the learning goals).

At the start of the TTX, all participants receive the same scenario information. After this, the exercise starts, and more role-specific information can be shared with individual participants. Again, scenario information or central dilemmas used in the TTX must logically follow from the RT phase. A TTX is always led and facilitated by an expert facilitator, trainer and observer for training and evaluation purposes. The minimum duration of a TTX is 3 hours. The TTX ends with a hot-wash to briefly let off steam and capture immediate improvement points.

4.3 Simulation (SIM)

The simulation is the most elaborate and challenging GT variant. It is intended for experienced CMTs who want to practice with evidence-based scenarios in a realistically simulated setting. In the interactive SIM variant, the entity's CMT experiences what it really means to be confronted with a crisis.

The goal of a SIM is to exercise and train crisis management skills (based on learning goals) under stress, by confronting team members with a realistic, hectic and unfolding crisis scenario. Under time pressure, the CMT members must determine their actions to mitigate the impact of the crisis. Detailed scenario information and events (injects), such as phone calls, emails, messages on social media channels and the news can be inserted in multiple ways, for instance by simulation tooling or counterplay.

There are two SIM subvariants:

- **A: Simulation without counterplay** – in this subvariant, static or pre-defined scenario injects are sent to the exercise participants through various (fictitious) channels (e.g. using simulation tools) from the exercise control cell or facilitator.
- **B: Simulation using counterplay** – this subvariant uses dynamic scenario injects that are sent to the participants from the exercise response cell. Counterplay events are based on actions performed by the CMT, in order to make the exercise more realistic. Also, this variant can be an unannounced exercise to boost realism and test reachability and attendance of crisis management personnel.

An exercise leader has the ultimate responsibility for the simulation. For both subvariants, the SIM set-up includes an exercise bubble that hosts the exercise participants, facilitator, trainer and observer. Also, technical and operational teams can be involved to train and practice team interaction. This can make counterplay very realistic, as it will be played by other incident teams or CERTs that are taking part in the training. The scenario injects and/or responses are provided to the exercise bubble(s) (plural, if multiple teams are involved) from the exercise control or response cell that is in a separate room or location.

The SIM B variant is the costliest one. As it is a very detailed scenario exercise, thorough facilitation, observation and response cell capabilities are needed, and tools and technologies will likely also be used to make the simulation as realistic as possible. The minimum duration is 4 hours and it ends with a hot-wash to briefly let off steam and capture immediate improvement points.

Please note that a successful SIM requires profound and meticulous preparation, execution and evaluation. Close collaboration with the entity's business and BCM team is required.

4.4 Overview of relative differences and similarities

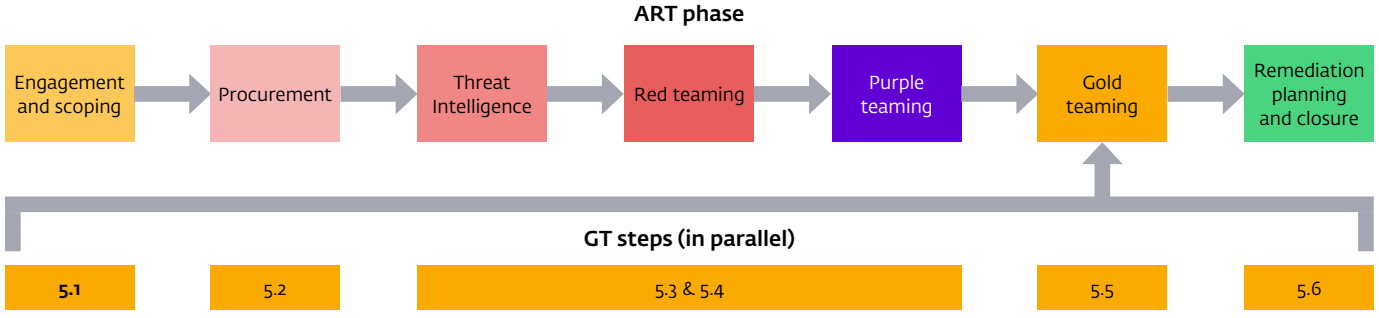
	WS	TTX	SIM A	SIM B
Purpose	Validate crisis management process and increase understanding of CMT roles.	Practice and train crisis management in a low-stress environment.	Exercise crisis management capabilities under pressure.	Exercise crisis management as realistic as possible.
Participants	Depending on learning goals.	CMT.	CMT.	CMT.
Complexity	Low.	Medium.	High.	Very high.
Relative investment	Low.	Medium.	High.	Very high.
Set-up	Discussion-based session (announced).	Paper or desktop-based exercise (announced).	Simulated exercise bubble(s) (announced or unannounced).	Simulated exercise bubble(s) + response cell (unannounced).
Roles	Led and facilitated by a facilitator/ trainer.	Moderated by a led facilitator and trainer / observer.	Exercise leader, facilitator(s), trainers(s) and observer(s).	Exercise leader, response cell members, facilitator(s), trainers(s) and observer(s).
Duration	Min. 2 hours.	Min. 3 hours.	Min. 4 hours.	Min. 4 hours.
Scenario-depth	Limited, high-level scenario.	Moderate, storyline based on central dilemmas and scenario injects.	In-depth, detailed (static) storyline and scenario injects.	In-depth, detailed (dynamic) storyline, scenario injects and response cell scripts.
Required maturity	Unexperienced CMTs or CMTs which have had personnel changes.	CMTs that already have some experience in crisis management.	Experienced CMTs.	Experienced CMTs.

For a full overview of all deliverables per variant please see section 6.

5 Detailed description of the gold teaming steps

This section of the GT guide uses six steps to chronologically describe the GT module all the way through:

- GT scoping (5.1).
- Staffing and procurement (5.2).
- Planning (5.3).
- Scenario development and preparation (5.4).
- Execution (5.5), and.
- Evaluation and improvement (5.6).



In addition to minimum requirements, milestones and tips are described per step to provide guidance to the CT and GT project team to help them work through GT module in a structured manner. While some of the steps can run in parallel, other should be closed deliberately using a go/no go meeting with the TCT to assure safety, quality and solid alignment with the RT phase and scenario of the ART-test.

Please note in the figure that the lead time of each step differs per variant.

5.1 Step 1: GT Scoping

For GT, scoping should be done well ahead of the actual start of the module, as part of the main 'engagement and scoping' ART phases. Please note that here the GT module specific scoping is meant and not the scoping of critical functions and systems as described in section 4.2 of the ART framework.

The very first step for the entity, is to define whether the organisation wants to include the GT module in their ART test. This should be concluded during the pre-launch meeting. An entity's CMT portfolio is in most cases not managed by IT security, even though this department is most likely driving an ART test within the entity. Therefore, this should be discussed with the CMT portfolio holder(s) in the board. Board-level approval, mandate and support is a necessity for GT, just like for the other modules in the ART-test.

There are several other points to consider when deciding to do a GT or not. A practical but important consideration is whether it fits in the CMT's exercise planning. Here, both frequency and scenario variation of CMT sessions play an important role as the CMT's exercise planning should be well-balanced in terms of time and content. The resources available for the GT should also be inventoried as part of the scoping. If an entity decides to include the GT module in the scope of the ART test, the next step is to the define a high-level objective and learning goals. Based on the objective and learning goals, maturity of the CMT and practical boundaries such as budget and other resources, the entity chooses which GT variant fits best: the WS, TTX or SIM A or B variant. The choice of variant is made in consultation between the CT and TCT and this is used as input for the procurement phase. The objective and learning goals, along with the variant, are later also documented and specified in the GT Plan.

GT Scoping milestones:

- Decision on whether to include a GT module in ART.
- High-level objective and learning goals for the GT.
- Select a GT variant based on the objective, learning goals and other practical considerations.

GT Scoping requirements:

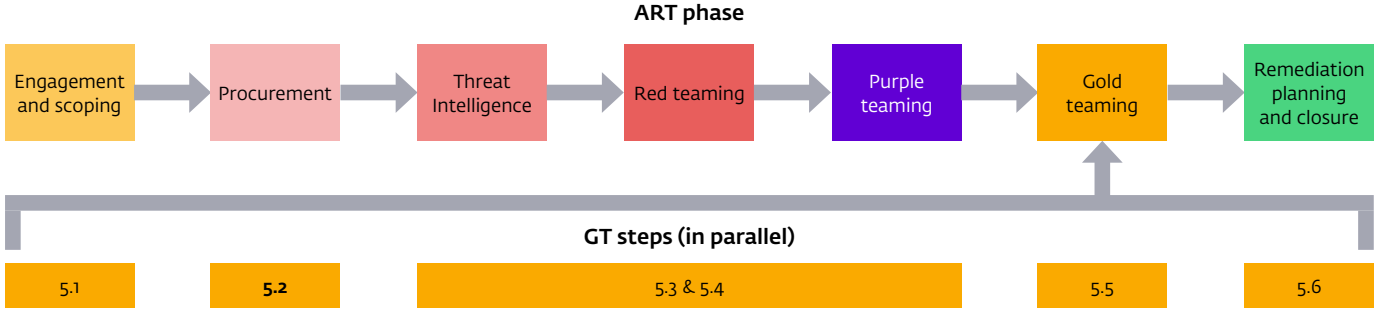
- Board-level approval, mandate and support.
- The GT variant is selected based upon a high-level objective and learning goals which are documented in a brief overview.

GT Scoping tips:

- If the CMT agenda is overly full, try using an existing training/exercise date to execute the GT instead. Make sure a good mix of scenario categories (physical, financial, legal, cyber, etc.) are trained throughout the year.
- Make sure learning goals align with the goals and objectives in the entities Educate, Train and Exercise (ETE) plan (in Dutch: Opleiden, Trainen & Oefenen), if available.
- In most cases, the entity's Business Continuity Management (BCM) team would be the right team to consult for the two beforementioned tips.

A successful GT module in which scope, quality and safety are all assured, requires specific skills and knowledge from a team of professionals, especially for the TTX and SIM variant. It is the entity's responsibility to compose the right team of professionals with the right capabilities to fully run the GT module. This is coordinated by a GT lead.

5.2 Step 2: Staffing and procurement



The GT lead is responsible for ensuring the success of the GT module at the tested entity. The GT lead must therefore be someone with strong project management skills, and preferably also with an affinity for crisis management. However, the GT lead should not be part of the CMT as participants in the GT module should not be involved in preparatory activities. The GT lead is part of the CT, to assure the connection and alignment between the RT phase and the GT assignment. The CT lead can also take on the role of GT lead, as long as this person has commitment from the crisis management portfolio holder in the board and this is the right person, with the right capabilities for the job. The CT remains overall responsible for the ART test.

An entity can decide to perform the GT module with internal or external resources. In the latter case, the entity procures a GTP. The decision to use internal or external resources is up to the CT in consultation with the TCT and is based on available expertise, means and resources needed to deliver the GT variant to achieve the objective and learning goals. If the entity decides to use its internal resources and capabilities, it is important to emphasise the number of staff-hours that go into the different steps of a GT module.

The GT project team (internal project team or a procured GTP) is responsible for the deliverables and organization that is required for the development, execution and evaluation of the GT module. This team must therefore have demonstrable experience and capabilities in:

- Project management.
- Crisis management and organizational resilience.
- Cyber security.
- Cyber scenario development (in collaboration with business, BCM and IT).

- Facilitation and session leading skills.
- Training and observation skills.
- Exercise leader skills (TTX and SIM).
- Response cell and counterplay skills (TTX and SIM).
- Evaluation and advisory skills (TTX and SIM).

The TCT provides guidance to the CT and GTP or internal project team throughout all the GT steps. The TCT's role is to assure that the GT runs according to the ART requirements in a safe manner. Therefore, all deliverables throughout the GT are shared with the TCT. Sufficient confidence from the CT and TCT in the content, capacity and expertise throughout the GT assignment is a key requirement.

Staffing and procurement milestones:

- The role of GT lead is assigned to a CT member.
- In case of internal assignment: dedicated and installed GT project team.
- In case of procurement: successful tendering procedure based on the GT minimal requirements.
- In case of procurement: signed contract between the entity and the GTP.

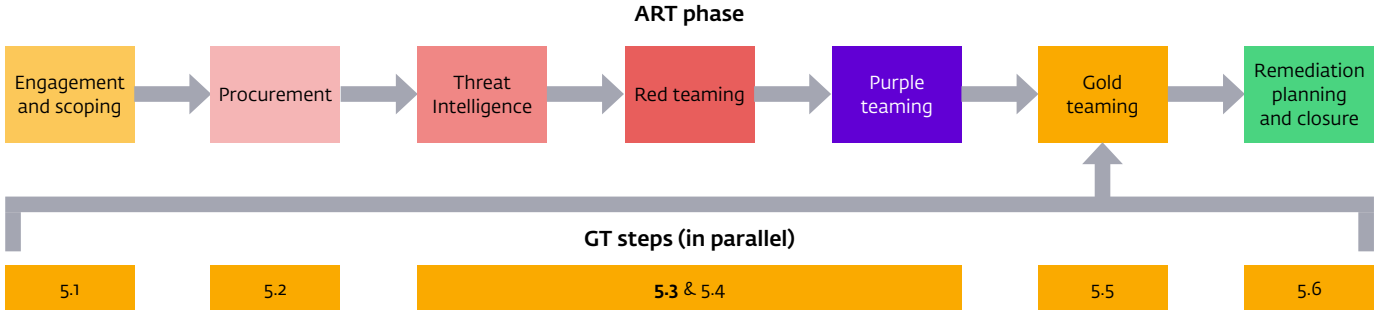
Staffing and procurement requirements:

- The GT lead is part of the CT and has the right capabilities and experience.
- Participants of the GT are not involved in preparatory activities.
- In case of internal assignment: the internal project team has the right (demonstrable) knowledge, experience and skills required for the chosen GT variant.
- In case of procurement: the procured GT team has the right (demonstrable) knowledge, experience and skills required for the chosen GT variant (through CV's and relevant project portfolio).

Staffing and procurement tips:

- If an entity chooses to perform the GT module with internal means, set up an internal project team in a timely fashion. Ensure the confidentiality of the GT.
- In case of procurement: start the procurement process well ahead of time. Timing is everything in GT to ensure connection with the RT phase. Give your GTP the opportunity to allocate resources and to start developing the GT module in a timely fashion.
- Also, run the procurement of the GTP in parallel with the RTP and TIP (if applicable). Some providers can offer services for more than one module, which can be beneficial in terms of recourses and alignment between different teams and modules.

5.3 Step 3: Planning



Once the project team has been composed, the GT planning step commences. This step formally begins with a GT kick-off meeting and should start in a timely fashion, preferable during the TI phase or early stages of the RT phase of the test. The kick-off meeting is held between the TCT, CT (at least the GT lead), RTP and GTP or internal project team to discuss the key content-related and practical matters.

These matters include:

- Learning goals.
- Timelines and deliverables.
- Project roles and responsibilities.
- Participants.
- Execution date.
- Set up of the GT.
- Central dilemmas for the High Level Scenario (HLS).
- Risk management (specifically for TTX and SIM).

The kick-off meeting participants should preferably also brain-storm about a high-level scenario and central dilemmas to build on the RT technical scenario. Naturally, all topics mentioned above can be prepared prior to the kick-off by the GTP or internal project team. In that case, the kick-off meeting is more validating in nature.

Subsequently, all key elements that lay the groundwork for the GT as discussed in the kick-off should be documented in a GT plan. Depending on the chosen variant and the set-up of the exercise, the plan should incorporate a number of elements focused on risk management in the GT exercise (specifically for TTX and SIM). This is to prevent exercise information from accidentally leaking out to people or personnel that are not part of the exercise, possibly creating a situation where exercise injects or information 'escape' into the wild. Thorough risk management prevents such escalations. This requires digital, physical and hierarchical containment measures to protect the confidentiality of the exercise. GT will then enable entities to practice their crisis management response in a controlled and safe setting.

It is important that the GT is planned not too long after the RT or purple teaming (PT) phase. The effectiveness (and connectedness with the RT phase) of the GT session will be enhanced if the 'pain' (findings) from the RT phase is still present. For example, if the RT provider simulated a ransomware scenario during the RT phase, the GT module might start as soon as possible after the ransom-ware has been 'deployed' on the targeted systems. Even if the RTP did not manage to reach the flags in the scenario, the GT scenario will assume that it did.

Optimal timing of the GT differs per test as it depends on the complexity of the test, findings and specific learning goals. Here, professional judgement is required from the GTP, CTL and TCT.

Planning milestones:

- Finalised version of the GT plan.
- Approval of the GT plan by the TCT and CT (go/no go).

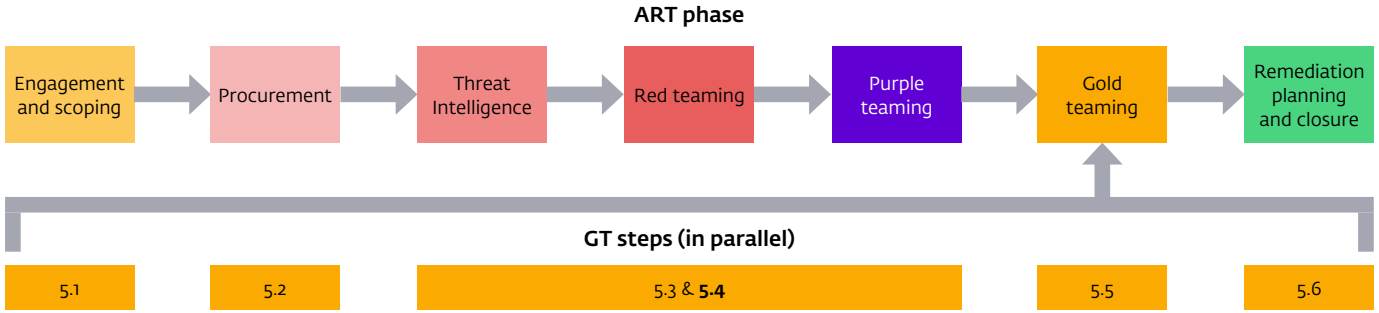
Planning requirements:

- GT kick-off meeting.
- GT plan, emphasis on connection between GT and RT, in both timing and content.

Planning tips:

- In case of procurement of a GTP, parts of the contract or proposal may be useful input for the GT plan.
- Include review and approval time for the TCT in timelines and planning.
- Take time for the kick-off meeting to ensure that all aspects (learning goals, timelines, etc.) thoroughly discussed to enable the GT project team to develop a plan. Ideally, the cornerstones of the scenario are also explored and defined during this meeting.
- As in the RT phase, it is highly recommended to plan weekly check-ins with the CT, TCT and GTP or internal project team to track progress, identify blockers and to give the CT the opportunity to make decisions regarding the GT. These meetings can be incorporated in the regular weekly update meetings as the monitoring of the progress for planning and execution of these modules run in parallel.
- The impact that the RT had on the organisation should be a factor in the timing of the GT. For example, in some cases the start of the GT should commence directly after the RT. While in other instances it is advisable to delay the start of the GT by a couple of weeks to achieve optimal learning. The ideal starting point of a GT will be determined in consultation with the CT, TCT and GTP.

5.4 Step 4: Scenario development and preparation



After the TCT and CT provide a 'go' on the GT plan, the GTP or internal project team starts developing all required GT materials. This includes all materials needed for delivering a successful GT on GT-day, such as:

- Facilitation/trainer runbook.
- Scenario event list, injects and event information.
- Simulators and tooling.
- Response cell playbook.
- Observation forms.
- Hot-wash questionnaire.

Materials differ in content and size for each GT variant. The WS variant requires less preparation than the TTX and SIM variants, as a high-level scenario to validate plans and a short script on how the session is structured could be sufficient. Naturally, the WS variant does not require simulators and tooling, observation forms or a hot-wash questionnaire. In addition to these materials, all practical matters must be prepared in this step, such as securing locations, required technology and tools, and arranging catering.

The foundation for the scenario was already created by the development of the HLS in the GT plan. In this step, the HLS evolves into a detailed master scenario event list (MSEL). An MSEL is a chronological timeline of scenario information and scripted events that will be injected into the TTX or SIM. These injects can be static in the TTX and SIM without counterplay. This means that the scenario has no or only very limited variations in the way in builds up to the end state.

If counterplay by a response cell is performed as part of a SIM (variant B), the MSEL and response cell playbook include dynamic events and responses that can be injected into the exercise. These can vary, based on the decisions, actions or requests from the CMT. A certain degree of improvisation will always be necessary as there are different storylines that can lead to the scenario end-state. Response cell capability therefore requires extensive experience.

For WS, TTX and SIM, the scenario must build upon (one of) the scenario(s) played in the RT phase. Thus, the GT scenario translates the technical implications of the RT phase to a strategic level, focusing on the organisational (reputational, operational, safety and security, financial and legal) impact of the findings of the ART test. By translating the technical findings into strategic impact in the GT scenario, the RT findings become tangible for senior management. The GT scenario should be developed under the assumption that the RT scenario is successful and the red team reached the flag. For example, if the RTP was unable to deploy ransomware in the RT phase, the starting point for the GT scenario is that ransomware deployment was successful. This way, the GT scenario remains threat intelligence-based.

For the sake of realism and in view of the evidence-based nature of GT, it is important that preparation and scenario development by the GTP or internal project team takes place in close collaboration with the other stakeholders, such as:

- Threat intelligence provider (TIP) and RTP (for relevant TI to be included, such as tactics, techniques and procedures [TTPs] and threat actor behaviour and details).
- BCM teams.
- IT departments (to enhance realism on technical and systems level).
- Business departments (to enhance realism on operational and business level).

In collaborating, please take into account the confidentiality principle. Finally, ensure that roles that will partake in the GT session are not involved in the development and preparation of the GT module in order to maximise the learning outcome.

Scenario development and preparation milestones:

- Finalised GT scenario (MSEL) that is accepted by the CT and TCT (go/no go).
- Finalised GT materials.
- All practicalities are arranged.
- Successful dry-run (for TTX and SIM).

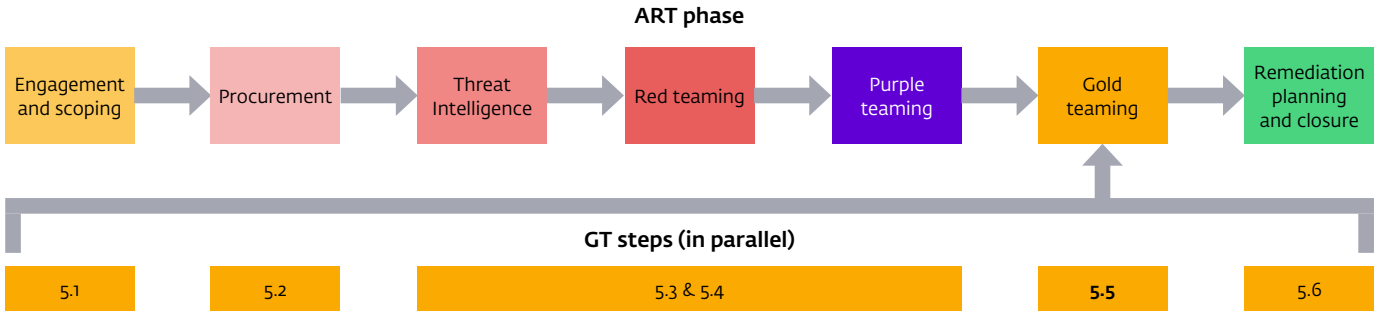
Scenario development and preparation requirements:

- The GT scenario is TI and evidence-based, and builds upon the scenario as emulated in the RT phase.
- The scenario is developed in close collaboration with the tested entity, TIP and/or RTP. CMT plans and procedures are consulted during the preparation.
- Execution of a dry run for the TTX and SIM variant to ensure sound GT execution on GT-day. The TCT can be present during the dry-run. Also, attendance of the TCT on GT-day is not mandatory but can be discussed if preferred by the CT or GTP.

Scenario development and preparation tips:

- Build the scenario from a certain end-state and include board-level dilemmas that align with the learning goals.
- Include documentation and procedures from the entity in the development and preparation.
- Check whether all technology and tools are working properly before execution (mandatory for TTX and SIM through a dry run).
- Participants, facilitators and trainers can experience a TTX or SIM session as particularly demanding. Make sure food and drinks are available and apply due care to the participants during an possibly after the exercise.

5.5 Step 5: Execution



After all the preparatory activities, the actual GT is executed on GT-day. Execution of a GT session can follow either the RT phase or the PT phase of an ART test. This may vary depending on the variant chosen, the weight of the findings from the RT phase and availability of resources. The CT consults with the TCT to determine what will be best.

GT-day itself should be facilitated tightly, based on a runbook and other exercise materials as defined in the section 5.4. The GT lead or head facilitator kicks off the GT session with an introduction, stressing that the GT session that the participants are about to take part in is TI and evidence-based (in other words: the scenario as played could happen in real life tomorrow!).

For the TTX and SIM variants, the practical GT set-up and rules of the road are also discussed prior to the GT session. This includes GT confidentiality, no-play situations and containment measures (physical, digital and/or hierarchical). Containment means: how to prevent scenario information from leaking out of the exercise bubble(s) on location, via digital communication channels and (hierarchical) escalation lines. Finally for all variants, the GT lead or head facilitator checks whether all participants are comfortable and ensures a safe learning environment.

The GT session then starts. The duration of the GT session is variable and should be determined by the CT in consultation with the TCT and GT project team based on the learning goals, exercise set up and complexity. The following minimal durations apply:

- WS: min. 2 hours.
- TTX: min. 3 hours (including introduction and hot-wash).
- SIM: min. 4 hours (including introduction and hot-wash).

It is advisable to divide the GT into rounds and take at least one short break.

There are always trainers and observers present during all variants of a GT session. For the WS variant, the facilitator can also take on the role of trainer and observer given the relative simple set up of this variant (if this person has the right capabilities).

After completion of the TTX or SIM variant of the GT session, it is advisable to hold a brief hot-wash. This way, participants can share their first experiences, let off steam and immediate improvement points can be captured. It is the facilitator's responsibility to conclude the GT positively but constructively.

Execution milestones:

- At the beginning of the execution of the GT-scenario, the scene is set through an introduction in such a way that participants feel the urgency and realism of the GT and the scenario.
- Successful delivery of a GT with enough observations to start developing an action list (for WS) observation report (for TTX) and an evaluation report (for SIM).
- All participants have had the opportunity to let off steam, share first impressions and immediate improvement points can be captured, all of which are documented.

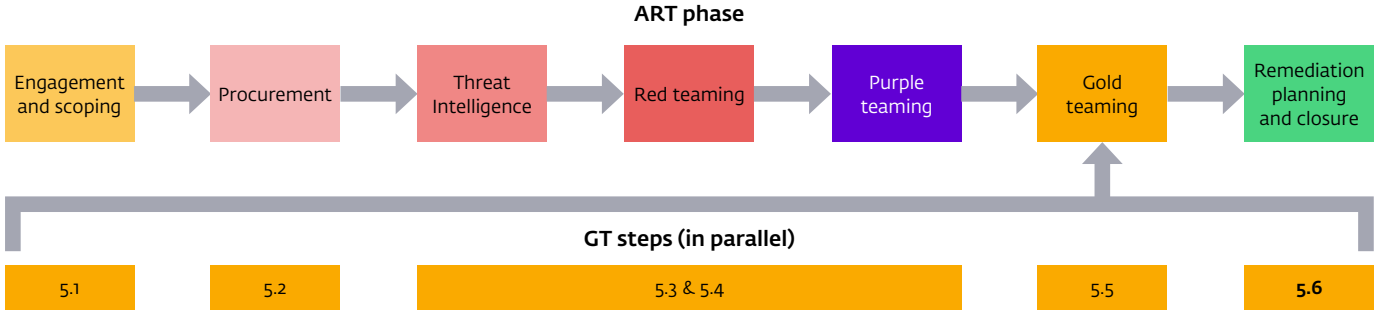
Execution requirements:

- During the introduction, the alignment and connection between the GT and RT modules of the ART test are made very clear. The difference between a regular CMT exercise and this GT (TI and evidence based) is made clear to participants, as this contributes to the sense of urgency and realism of the GT.
- The GT session is observed for reporting and evaluation purposes.
- The GT session concludes with a hot-wash to make sure the GT finishes in a positive and constructive way and immediate improvement points are captured (TTX and SIM).

Execution tips:

- The head facilitator may briefly give the floor to the RT team after the GT session so that they can convey the potential impact of the findings from the RT phase. In most cases, the RT team is particularly able to convincingly describe what they could have done (e.g. shut down operations, deploy ransomware, adjust transaction data) and what the consequences of their actions would have been. Don't do this during the introduction of the GT as this might give away the scenario.
- Make sure the roles needed for the GT are present (online or physically, depending on the GT set-up), but do not let the group get too big. Also, attendance of the TCT on GT-day is not mandatory but can be discussed if preferred by the CT or GTP.

5.6 Step 6: Evaluation and improvement



After the execution step, the CMT's efforts and capabilities, crisis management processes, procedures, tools and formats are evaluated. The observations serve as the main input in this final step. The findings from the hot-wash are also taken into consideration. The learning goals as defined in the plan are the common thread in the evaluation. Naturally, additional observations and analyses can be included.

The evaluation output depends on the GT variant. The more complex the GT, the more extensive the evaluation.

- For the WS variant, an overview of actions or points for improvement regarding crisis management documentation and processes.
- For the TTX variant, an observation report including observations and lessons identified or points for improvement.
- For the SIM variant, an evaluation report including observations, analysis and lessons identified or points for improvement.

For the TTX and SIM variant, evaluation findings and points for improvement are presented to the crisis management owner(s) at the board level. It is subsequently advisable to create a plan to arrange ownership and implementation of improvements. Please note that actual improvement following evaluation efforts is out of scope of the ART test.

Finally, it is important that the GT evaluation is comparable to previous crisis management evaluations carried out by or for the entity. It is only through comparable evaluations and corresponding evaluation criteria that improvement and development can be objectively determined and monitored over time.

Evaluation and improvement milestones:

- Finalised report, shared and accepted by the CT and TCT (go/no go).
- Presentation of evaluation and points for improvement to the board (for TTX and SIM).

Evaluation and improvement requirements:

- The evaluation and associated report are based on the learning goals as defined in the GT plan.
- The GT evaluation enables comparability with previous crisis management evaluations for the entity.
- The evaluation and points for improvement are shared with the CMT portfolio holders in the board (for TTX and SIM).

Evaluation and improvement tips:

- After the PT and evaluation of the RT report, a board meeting is held to communicate the results and impact of the test. If a GT module is part of the test, this meeting can also be used to share evaluation results and points for improvement from the GT with the CMT portfolio holder on the board.

6 Overview of requirements

The requirements presented in the paragraphs below follow from the text in this guide and serve as a summary. In addition to these requirements, the core principles of GT as described in section 3 should always be applied.

A safe learning environment must be created and maintained at all stages of the module to develop and enhance crisis management skills through GT. A key requirement is that the CT and TCT have sufficient confidence in safety, capacity and expertise throughout the GT assignment. In case the TCT and/or CT feels the test is unsafe or has substantial doubts about the expertise of the GT project team, the module can ultimately be stopped prematurely and the ART label can be removed from the module as a last resort. This means the module will not be signed off in the attestation document.

6.1 Required deliverables

	WS	TTX	SIM
Scoping	Overview of high level objective and learning goals.	Overview of high level objective and learning goals.	Overview of high level objective and learning goals.
Procurement and staffing	Not applicable.	Not applicable.	Not applicable.
Planning	GT plan (go/no go).	GT plan (go/no go).	GT plan (go/no go).
Scenario development and preparation	Brief runbook. HLS (go/no go). Observation form.	Runbook. MSEL and injects (go/no go). Observation forms. Hot-wash questionnaire.	Runbook. MSEL and injects (go/no go). Simulators and tooling. Response cell playbook. Observation forms. Hot-wash questionnaire.
Execution	Filled observation forms.	Filled observation forms.	Filled observation forms.
Evaluation and improvement	Overview of actions or improvement points.	Observation report.	Evaluation report.

6.2 Required expertise

	WS	TTX	SIM
Roles	GT Lead. Project team for preparation and organisation. Facilitator/observer.	GT Lead. Project team for preparation and organisation. Exercise leader. Facilitator. Trainer/observer.	GT Lead. Project team for preparation and organisation. Exercise leader. Facilitator(s). Trainer(s). Observer(s). Response cell members.
Knowledge	Project management. Crisis Management and organisational resilience. Cyber security.	Project management. Crisis Management and organisational resilience. Cyber security. Evaluation.	Project management Crisis Management and organisational resilience. Cyber security. Evaluation.
Skills	Facilitation and session leading. Observation skills.	Exercise leader skills. Facilitation skills. Training skills. Observation skills. Evaluation skills. Advisory skills.	Exercise leader skills. Facilitation skills. Training skills. Observation skills. Response cell and counterplay skills. Evaluation skills. Advisory skills.

6.3 Misc general requirements

	WS	TTX	SIM
Scoping	Board level approval, mandate and support.	Board level approval, mandate and support.	Board level approval, mandate and support.
Procurement and staffing	GT lead is part of CT. Participants are not involved in preparation. All roles are assigned. Roles have the required knowledge and skills.	GT lead is part of CT. Participants are not involved in preparation. All roles are assigned. Roles have the required knowledge and skills.	GT lead is part of CT. Participants are not involved in preparation. All roles are assigned. Roles have the required knowledge and skills.
Planning	GT kick-off meeting. GT close after RT/PT.	GT kick-off meeting. GT close after RT/PT.	GT kick-off meeting. GT close after RT/PT.
Scenario development and preparation	Scenario is TI and evidence based.	Scenario is TI and evidence based. Preparation in close collaboration with entity, RTP/TIP. Execution of a dry-run prior to GT-day.	Scenario is TI and evidence based. Preparation in close collaboration with entity, RTP/TIP. Execution of a dry-run prior to GT-day.
Execution	Min 2 hours. Alignment with RT as part of ART is made clear intro.	Min 3 hours. Alignment with RT as part of ART is made clear intro. Concludes with hot-wash.	Min 4 hours. Alignment with RT as part of ART is made clear intro. Concludes with hot-wash.
Evaluation and improvement	Based on learning goals.	Based on learning goals. Enables comparability. Shared with the board.	Based on learning goals. Enables comparability. Shared and presented to the board.

Annex: Abbreviations

ART	Advanced Red Teaming
BCM	Business Continuity Management
CERT	Computer Emergency Response Team
CMT	Crisis Management Team
CT	Control Team
CTL	Control Team Lead
DNB	Dutch Central Bank, DeNederlanscheBank
GT	Gold Teaming
GTP	Gold Teaming Provider
HLS	High Level Scenario
MSEL	Master Scenario Event List
PT	Purple Teaming
QA	Quality Assurance
RT	Red Teaming
RTP	Red Teaming Provider
SIM	Simulation exercise
TCT	DNB Test Cyber Team
TI	Threat Intelligence
TIP	Threat Intelligence Provider
TTP	Tactics, Techniques and Procedures
TTX	Table Top Exercise
WS	Walk-through Session

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

Follow us on:

DeNederlandscheBank
EUROSYSTEEM