ART Service Procurement Guide

for the financial sector

DeNederlandscheBank

EUROSYSTEEM

Contents

1 About this guide

This document provides an overview of all requirements, steps, and considerations for procuring service providers for an ART test. These providers include the Threat Intelligence Provider (TIP), Red Team Provider (RTP), and Gold Team Provider (GTP) (if applicable). This document describes the procurement process, the minimum requirements for service providers, and guidance regarding the procurement of service providers.

1.1 Purpose of this guide

The purpose of this document is to provide guidance on the successful procurement of service providers for an ART test, and to clarify the minimum requirements that these service providers should meet. This document addresses the procurement of the threat intelligence provider (TIP), red team provider (RTP), and optionally the gold team provider (GTP).

The ART test follows an integrated flow in which TI informs realistic RT scenarios, and RT findings may subsequently be translated into GT scenarios that test the institution's strategic, operational and crisis management response. The procurement process aims to mitigate risks by selecting TIP, RTP and GTP that adhere to strict standards of competence, ethics, and confidentiality. By doing so, it creates standards so that the test reflects genuine threat scenarios, supports robust risk management, and provides actionable insights to strengthen the entity's cyber resilience.

This guide is part of the ART framework as published by De Nederlandsche Bank 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)
- TCT or authorities involved in the ART test

1.3 Legal and disclaimer

This document is intended for institutions that plan to use the ART framework for conducting an ART test in the Dutch financial sector. 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 Interpretation of the guide

This guide sets out the general principles, minimum requirements and practical guidelines for service provider procurement in ART. It is not intended to provide an absolute metric for determining whether a provider meets the requirements in every possible case.

ART tests are context specific. Procurement decisions may therefore require professional judgement based on the scope, selected variants, maturity of the institution, available provider market and specific risk considerations.

The requirements in this guide are intentionally designed with sufficient room to reflect that reality. Where uncertainty exists about the interpretation or application of these requirements, the TCT should be consulted at an early stage to discuss the specific case and agree on an appropriate way forward.

1.5 Role of the TCT, minimal requirements and attestation

To set up and execute an ART test, the procurement of a TIP, RTP, and GTP (if applicable) is required. These service providers carry out the TI module, RT module, and/or GT module in the ART test. To ensure that these modules are performed according to the standards and quality required by the ART framework, the TCT is present.

The TCT will be present throughout all phases of the test. At critical moments in the service provider procurement steps, the TCT is there to ensure that the service provider procurement is executed following the requirements as presented in the ART framework and as detailed in this guide.

All TCT involvement will always happen in close collaboration with the Control Team.

Next to the quality assurance (QA) role, the Test Manager (TM) is a neutral sparring and guiding partner for the CTL who holds the ultimate responsibility for the ART test within the institution. If the test has been carried out in accordance with the requirements of the ART framework, the TCT will provide the institution with an attestation document concluding the test.

2 Introduction

2.1 What is the service provider procurement process in ART?

The service provider procurement within the ART framework is a critical step in the preparation phase, designed to ensure that only highly competent providers are procured for the test. This process involves thorough due diligence by the CT and CTL to validate that providers meet stringent requirements on skills, certifications, independence, and risk management, as outlined in this ART Service Procurement Guide. By doing so, the process mitigates certain operational and security risks inherent in testing live production systems and improves that the intelligence-led scenarios and red team/gold team activities are executed to the highest professional standards.

Where GT is included, the procurement process should also ensure that the GTP is able to translate RT outcomes into realistic crisis management exercises, so that technical findings are connected to organisational decision-making and resilience. Ultimately, the procurement process underpins the credibility, safety, and learning value of the ART test, ensuring that the entity can confidently assess and enhance its resilience against sophisticated cyber threats.

2.2 What is the purpose and goal of the service provider procurement process?

The purpose of the service provider procurement process is to safeguard the integrity, quality and realism of the exercise by selecting providers with suitable and proven expertise, robust methodologies, and strong ethical standards.

3 Core principles of service provider procurement

The procurement of service providers within the ART framework should follow principles that ensure quality, integrity, and safety throughout the test. These principles guide the selection and engagement of Threat Intelligence Providers (TIP), Red Team Providers (RTP), and Gold Team Providers (GTP).

3.1 Safety and risk management

During the entire ART process, the CTL and involved providers must prioritize operational safety and risk mitigation. Providers should demonstrate strong security controls and governance measures to prevent unintended disruptions or data breaches during the test.

3.2 Competence and professional standards

Providers should demonstrate their experience and expertise in delivering intelligence-led testing and, where applicable, crisis management exercises. They must provide written evidence that they meet the applicable requirements, such as relevant references, CVs, certifications and documented methodologies.

For more information on the requirements and expected evidence per Service Provider, see chapter 7.

3.3 Independence and objectivity

Providers should operate in a way that avoids conflicts of interest and ensures impartiality. An example is when TIP, RTP, and GTP belong to the same organization, a clear separation of roles and responsibilities and strict internal segregation of information sharing within the engagement is required to maintain integrity.

3.4 Confidentiality and ethical conduct

All providers must adhere to strict confidentiality protocols and ethical standards. Sensitive information obtained during the test should only be used for its intended purpose and securely destroyed after completion. It is the responsibility of the CTL to agree with the providers to be contracted which activities, methods and boundaries are considered acceptable within the ethical limits of the ART test. These agreements should be clearly documented before the relevant activities start.

3.5 Alignment with ART objectives

Providers should demonstrate flexibility and collaboration to ensure their methodologies and deliverables align with the ART framework's learning goals. This includes adapting threat intelligence, attack scenarios, and crisis exercises to the agreed scope. Alignment should be maintained across the full chain from TI to RT and, where applicable, GT. This means that threat intelligence should inform RT scenario development, and RT outcomes should provide evidence-based input for GT scenario design.

3.6 Transparency and accountability

The procurement process should be documented thoroughly, including evaluation criteria, decisions, and approvals. Providers must commit to clear reporting and communication throughout the engagement.

These principles ensure that the procurement process supports a controlled, realistic, and high-quality ART test, safeguarding both the institution and the integrity of the framework.

4 Stakeholders and roles & responsibilities

Clear roles and responsibilities are essential for a controlled and successful procurement process within the ART framework. Each stakeholder has defined tasks to ensure compliance, confidentiality, and alignment with ART objectives.

4.1 Control team

The Control Team, led by the CTL, represents the institution and is responsible for managing the entire procurement process. Acting as the central coordinator, the CT ensures that the ART test aligns with organizational objectives and regulatory requirements. The CT defines the scope of the test, prepares procurement documentation, and evaluates providers against the ART requirements. It also manages confidentiality and risk throughout the engagement.

Responsibilities:

- Define scope, learning objectives, and module variants in consultation with the TCT.
- Prepare procurement specifications or RFPs detailing requirements for TIP, RTP, and GTP.
- Conduct market engagement, evaluate proposals, and shortlist providers based on competence and independence.
- Perform due diligence, validate compliance evidence, and maintain full documentation for audit purposes.
- Act as the primary point of contact for providers and the Test Manager during procurement and planning.

4.2 Test Manager

The Test Manager (TM), appointed by the TCT, acts as the quality assurance authority for the ART test. The TM reviews the proposed provider against the ART requirements and provides either a non-objection or a no-go. The TM does not provide commercial approval, select providers on behalf of the institution, or influence commercial negotiations. The CTL remains ultimately responsible for the procurement decision within the institution.

Responsibilities:

- Reviews proposed providers and provides a non-objection or no-go.
- Neutral sparring and guiding for the CTL.
- Reviews compliance documentation, including CVs, certifications, and insurance coverage.
- Monitors adherence to ART principles and confidentiality obligations throughout planning and execution.
- Provides guidance on governance and risk management without influencing commercial negotiations.

4.3 Threat intelligence provider

The TIP delivers actionable threat intelligence that forms the foundation of the ART test. It is responsible for collecting and analysing intelligence based on the agreed TI variant (Basic, Extended, or Full) and producing a (targeted) threat intelligence report (TIR or TTIR). Depending on the variant to be executed, the TIP can be resourced internally or externally. In either case, the resources need to uphold the proper requirements and validation of such by the CTL should be performed. The TIP must ensure that intelligence is accurate, relevant, and aligned with ART objectives, while maintaining strict confidentiality.

Responsibilities:

- Collect and analyse threat intelligence based on the agreed TI variant (Basic, Extended, or Full).
- Produce a threat intelligence report (TIR) or targeted threat intelligence report (TTIR) including threat actor profiles, TTPs, and realistic attack scenarios.
- Ensure methodologies align with ART principles and confidentiality requirements.
- Provide qualified personnel, including a threat intelligence manager with sector knowledge and a multi-disciplinary team skilled in OSINT, HUMINT, and technical analysis.
- Maintain secure handling and destruction of sensitive data after the test.
- Collaborate with the RTP for scenario development and, where GT is included, provide relevant context to support the translation of TI and RT outputs into GT scenario material while preserving independence and confidentiality.

4.4 Red team provider

The RTP executes intelligence-led attack scenarios to assess the institution's resilience. It develops the red team test plan (RTTP) based on TI findings and conducts red teaming activities ethically and securely. The RTP must adhere to ART rules of engagement and deliver a comprehensive red team test report (RTTR) summarizing findings and recommendations.

Responsibilities:

- Develop a RTTP based on TI findings and agreed RT variant (Assumed Compromise, End-to-End Simulation, or Scenario X).
- Execute red teaming activities ethically and in compliance with ART rules of engagement.
- Maintain detailed logs of all actions and provide regular progress updates to the CT and TM.
- Deliver a comprehensive RTTR summarizing findings, impact, and recommendations, and document RT findings in a way that enables their translation into GT scenarios where GT is included.
- Lead and perform the PT session(s), depending on the selected variant for the PT module.
- Ensure confidentiality and secure handling of sensitive data throughout the engagement.
- Provide a qualified red team test manager and a multi-disciplinary team with expertise in exploit development, social engineering, and vulnerability analysis.

4.5 Gold team provider

The GTP designs and facilitates crisis management exercises to validate organisational resilience. It creates realistic, evidence-based scenarios based on TI context and RT findings, translating technical compromise paths into strategic, operational and crisis management consequences. The GTP may be the same provider as the RTP or a separate provider. Where the GTP and RTP are different parties, they should exchange the information necessary to develop realistic GT scenarios, while respecting agreed confidentiality, segregation and need-to-know principles. The GTP delivers evaluation outputs that help the institution improve its strategic response capabilities.

Responsibilities:

- Develop a gold team test plan (GTTP) aligned with the selected GT variant (Walk-through, Tabletop, or Simulation).
- Create realistic, evidence-based scenarios that use TI context and RT findings as input and translate technical compromise paths into strategic, operational and crisis management implications, including by coordinating with the RTP when the RTP and GTP are separate providers.
- Facilitate the gold team session and ensure a safe learning environment for participants.
- Deliver evaluation outputs such as an action list, observation report, or full evaluation report depending on the chosen variant.
- Implement containment measures to prevent leakage of scenario details before execution.
- Provide skilled facilitators, trainers, and observers with experience in crisis management and organizational resilience.

5 Service provider procurement variants

Choosing how to procure service providers is an important decision in the ART framework. The right approach depends on your organization's experience, resources, and learning goals.

5.1 Single provider variant

In this variant, one external provider is contracted to deliver multiple ART modules, typically Threat Intelligence and Red Teaming, and optionally Gold Teaming. All services are consolidated under a single organisation, which means the provider is responsible for intelligence development, test execution and, where applicable, the translation of RT outcomes into GT exercises. This structure reduces the number of contractual agreements and simplifies communication because the institution interacts with one primary point of contact. The provider manages internal segregation between its teams to ensure independence between modules.

Key Considerations:

- Independence must be guaranteed through strict internal segregation between TI, RT and, where applicable, GT teams.
- Risk concentration is high; failure of one provider impacts the entire test.
- Quality assurance depends on the provider's ability to deliver all modules at the required standard.
- Governance requires strong oversight to monitor segregation and confidentiality.

Key Decisions:

- Validate provider capability for all selected modules, including the ability to translate RT outcomes into GT exercises where GT is included.
- Include contractual clauses enforcing separation of roles and confidentiality.

5.2 Multi providers variant

The multi providers variant involves engaging separate providers for each module: one for TI, one for RT, and optionally one for GT. Each provider focuses exclusively on its area of expertise, which allows for specialized delivery of services. This structure creates clear separation between modules and ensures that intelligence gathering and attack execution are performed independently. The institution manages multiple contracts and coordinates timelines and deliverables across providers.

Key Considerations:

- Coordination effort is significant; multiple providers require robust planning and integration.
- Budget impact can be higher due to multiple contracts and management overhead.
- Governance must ensure alignment of timelines and deliverables across providers.

Integration risk may arise if TI findings are not translated into clear, executable RT scenarios, if RT findings are not prepared for GT scenario design where applicable, and if handover responsibilities are not explicitly agreed.

Key Decisions:

- Select providers with proven collaboration experience.
- Define integration points and communication protocols early, including TI to RT and, where applicable, RT to GT handover points.

5.3 Hybrid variant

The hybrid approach combines internal and external resources. For example, the institution may use its internal team to deliver Basic TI while contracting an external RTP or GTP. This variant integrates internal capabilities with external expertise, allowing the institution to maintain control over certain activities while outsourcing others. Internal teams must meet ART competency requirements and adhere to confidentiality protocols.

Key Considerations:

- Internal capability must meet ART competency requirements.
- Confidentiality controls are critical to prevent leaks from internal teams.
- Bias risk exists if internal teams are too close to systems being tested.
- Resource load increases due to managing both internal and external roles.

Key Decisions:

- Validate internal team qualifications and independence.
- Ensure segregation between internal and external responsibilities and define how outputs move from TI to RT and, where applicable, from RT to GT.

Variant	Characteristics	Considerations	Decision
Single provider	■ One provider: TI + RT (+ GT) ■ Simple coordination	■ Independence between phases ■ Risk concentration ■ Quality assurance ■ Governance	■ Validate capability ■ Add segregation clauses
Multi providers	■ Separate providers: TI, RT, GT ■ Specialized expertise	■ Coordination effort ■ Possibly higher cost ■ Integration risk ■ Governance	■ Choose experienced providers ■ Define handover points
Hybrid	■ Internal + external mix ■ Example: internal TI, external RT and external GT	■ Internal competence ■ Confidentiality ■ Bias risk ■ Resource load	■ Check internal competence ■ Enforce confidentiality

6 The service procurement steps

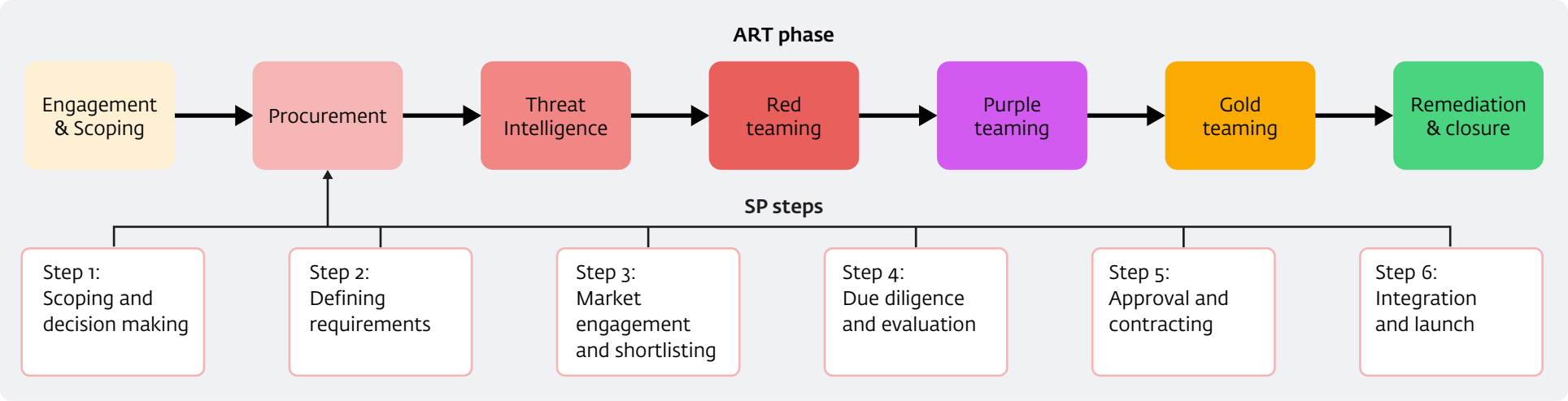
This chapter describes the service provider procurement process within the ART framework. The procurement of service providers – Threat Intelligence Provider (TIP), Red Team Provider (RTP), and, where applicable, Gold Team Provider (GTP) – is a mandatory preparatory activity within the ART framework.

A structured procurement approach is essential to safeguard the integrity of the test and to mitigate risks associated with testing on live production systems. This process ensures that providers meet the required standards for competence, independence, and security.

The procurement phase begins after the scope of the ART test has been defined and approved. It consists of six steps:

- Step 1: Scoping and decision making
- Step 2: Defining requirements
- Step 3: Market engagement and shortlisting
- Step 4: Due diligence and evaluation
- Step 5: Approval and contracting
- Step 6: Integration and launch

Each step is described in detail on the next pages.



Step 1: Scoping and decision making

The scoping phase forms the foundation of the ART test. During this phase, the Control Team (CT), in consultation with the TCT, identifies the critical or important functions (CIFs), the systems supporting these functions, and the "flags" that represent the Red Team's objectives. These elements are documented in the Scope Specification Document (SSD), which serves as the reference point for the remainder of the process.

In addition to defining the technical scope, the CT determines which modules the entity wants to include in the test, and with which variant. Choices made at this stage influence the complexity, duration and resource requirements of the test and should be aligned with the institution's learning objectives, maturity level and available capabilities. The TCT has an advisory role in this process, but the final decision on the scope and overall size of the ART test remains with the institution itself.

Milestones

- Scope and learning objectives defined and documented.
- Critical systems, CIFs and flags identified and recorded in the SSD.
- Module variants selected for TI, RT and (if applicable) GT.
- Confidentiality measures established (e.g. code name, access restrictions).
- C level approval and TCT validation obtained.

Deliverables

- Approved Scope Specification Document (SSD).
- Confirmed module configuration and high level planning parameters.

Step 2: Define requirements

After the scope and module variants have been agreed, the CT determines the minimum requirements that prospective service providers must meet. These requirements ensure that the TIP, RTP and GTP possess the appropriate expertise, experience, independence and security capabilities to support a safe and high quality ART test.

The requirements are formalised in a procurement specification or Request for Proposal (RFP). These documents outline expectations regarding technical competence, team composition, methodologies, quality standards and confidentiality obligations.

Milestones

- Procurement specification or RFP completed and aligned with ART framework and addenda.
- Minimum role qualifications, team requirements and competence criteria established.
- Security, confidentiality and ethical requirements defined.

Deliverables

- Finalised RFP including requirements for:
  - TIP: Threat Intelligence Report (TIR/TTIR)
  - RTP: Red Team Test Plan (RTTP) and Red Team Test Report (RTTR)
  - GTP: Gold Team Test Plan (GTTP) and evaluation report

Please refer to the applicable ART service provider requirements in chapter 7.

Back to overview service procurement steps

Step 3: Market engagement and shortlisting

Market engagement involves identifying potential service providers and assessing whether they can meet the requirements established in Step 2. Providers are invited to respond to the RFP and to demonstrate compliance with ART expectations. Their submissions typically include references, CVs, certifications and descriptions of relevant experience.

Subsequently, the CT performs an initial evaluation and documents the outcome. Providers that meet the minimum requirements are shortlisted and discussed with the Test Manager.

Milestones

- RFP shared with identified providers.
- Responses and supporting documentation received and reviewed.
- Evaluation completed using predefined criteria (competence, independence, capacity, security).
- Shortlist prepared and reviewed with the Test Manager.

Deliverables

- Documented evaluation results.
- Shortlist of providers meeting minimum ART requirements.

Step 4: Due diligence and evaluation

In the due diligence phase, the CT verifies that shortlisted providers meet the technical, operational and governance standards required for participating in an ART test. This includes assessing the qualifications and experience of proposed team members, reviewing evidence of independence and insurance coverage, and evaluating the methodologies used for TI, RT and GT.

Security and confidentiality measures are examined to ensure appropriate handling of sensitive information throughout the test. The CT documents its findings and addresses any identified risks.

Milestones

- Verification of provider qualifications and experience completed.
- Methodologies assessed against ART principles.
- Security and confidentiality controls reviewed.

Deliverables

- Due diligence report including evaluation outcomes.
- Recommendation by CT on providers suitable for contracting.

Back to overview service procurement steps

Step 5: Approval and contracting

Following execution of the due diligence, the CT shares the due diligence report and the evaluation outcomes with the Test Manager. Once the Test Manager has provided a non-objection, the CT can finalise the contracting documents with the provider(s).

Contracts must clearly outline the roles and responsibilities of each provider, define expectations regarding deliverables, and include provisions for confidentiality, data protection, intellectual property, security requirements and exit procedures. All contractual documentation is retained for audit and regulatory purposes.

Milestones

- Test Manager provides a non-objection for contracting the selected provider.
- Contract terms agreed and finalised with selected providers.
- NDAs and confidentiality commitments completed.

Deliverables

- Signed contracts including roles, responsibilities and deliverables.
- Documentation of contractual safeguards (e.g. confidentiality, IP, continuity).

Step 6: Integration and launch

After contracting, the selected providers are integrated into the ART test structure. This step begins with a joint launch meeting involving the CT, Test Manager and all engaged providers.

The purpose of the launch meeting is to confirm roles and responsibilities, review deliverables, align planning and reinforce confidentiality and risk management measures. Coordination between the TIP, RTP and (if applicable) GTP is established, particularly for the transition from TI to RT and the subsequent preparation for GT. The integration plan should define not only the TI-to-RT handover, but also how RT findings, attack narratives and impact evidence will be translated into GT scenario material, without disclosing unnecessary sensitive details.

Milestones

- Launch meeting held with all providers and stakeholders.
- Roles, planning and communication structure confirmed.
- Confidentiality and security protocols reinforced.

Deliverables

- Agreed integration plan for TIP → RTP → GTP handover, including how RT outputs will be translated into GT objectives, injects and evaluation focus areas where GT is included.
- Finalised meeting schedule, escalation paths and reporting arrangements.

Back to overview service procurement steps

7 Requirements providers

This chapter outlines the minimum requirements for Threat Intelligence Providers (TIP), Red Team Providers (RTP), and Gold Team Providers (GTP) engaged in ART tests. Providers must demonstrate capability, experience, and compliance with these requirements during procurement. Evidence should include references, CVs, certifications, and documented methodologies.

7.1 Threat Intelligence Provider Requirements

7.1.1 General requirements

Category	Requirements
Organisational requirements	■ Demonstrably relevant portfolio of comparable threat intelligence assignments related to red-team testing with at least **two references** from comparable threat intelligence engagements. ■ Capacity to form a TI team of at least two people, with additional capacity available if needed. ■ Adequate indemnity insurance in place to cover activities which were not agreed upon in the contract and/or which stem from misconduct, negligence, etc. ■ No previous or current services delivered for the entity, that would present a conflict of interest for the Service Provider when conducting an ART test.
Technical requirements	■ Access to up-to-date threat actor databases and TTP repositories. ■ Having access to (private or commercially available) threat intelligence databases, at minimum containing up to date threat actor profiles and their TTPs. ■ Ability to perform (targeted) threat intelligence analyses. ■ Ability to demonstrate active subscriptions or proprietary intelligence feeds. ■ Structured methodology for intelligence collection, validation, and reporting.

Category	Requirements
Deliverables	■ Capability to produce a Threat Intelligence Report (TIR) or Targeted Threat Intelligence Report (TTIR) including: – Executive summary – Business overview – Threat landscape – Threat Actor selection – Attack scenarios. ■ Ability to provide actionable intelligence aligned with ART learning goals.
Security and governance	■ Demonstrable ISMS or equivalent security framework. ■ Secure handling and destruction of sensitive data post-test. ■ Clear protocols for handling sensitive data and secure destruction post-test. ■ Compliance with confidentiality and GDPR requirements.

7.1.2 Basic threat intelligence variant

Category	Requirements
Team requirements	■ 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 Guide. ■ 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.

7.1.3 Extended Threat intelligence variant

Category	Requirements
Team requirements	■ 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 team should have appropriate recognised qualifications and certifications for threat intelligence. ■ The individuals have worked at least three years at the financial institution or a similar institution. ■ The individuals have more than 2 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 CTL must discuss the suitability of the TI provider.

7.1.4 Full threat intelligence variant

Category	Requirements
Organisational requirements	■ 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.
Team requirements	**Threat intelligence 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. **Threat intelligence 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.

7.2 Red Team Provider Requirements

Category	Requirements
Organisational requirements	■ Demonstrably relevant portfolio of comparable threat intelligence assignments related to red-team testing with least three references from comparable Red Team engagements. ■ Capacity to form a Red Team of at least three persons, with additional capacity available if needed. ■ Adequate indemnity insurance in place to cover activities which were not agreed upon in the contract and/or which stem from misconduct, negligence, etc. ■ No previous or current services delivered for the entity, that would present a conflict of interest for the Service Provider when conducting an ART test.
Team requirements	**Red Team Manager** ■ Sufficient experience in Red Team Testing. At least three years of experience in Red Teaming, with at least one year of experience of managing intelligence-lead red teaming. ■ Up-to-date CV to be provided to the entity, specifically in delivering red team testing activities. ■ Background checks on the Red Team Manager are conducted by the RT provider (as a minimum), including those required by the national authorities. ■ Able to explain advanced, technical RT subjects to both technical personnel (such as the members of the BT) and to non-experts in an understandable manner, guiding the CT through the RT phase in a clear manner. ■ Understands core financial processes, critical systems (such as payment and settlement platforms), sector-specific regulations and challenges, and common cyber threat scenarios affecting the financial sector. ■ Extensive project management capabilities, including the ability to organise its activities effectively, coordinate with relevant stakeholders, and deliver its contributions within agreed timelines and parameters.

Category	Requirements
Team requirements	**Red Team members** ■ Sufficient experience in Red Team Testing. At least two years of experience in Red Teaming. ■ Ideally, the Red Team should have experience in carrying out intelligence-led red team tests. ■ Up-to-date CV to be provided to the entity, specifically in delivering red team testing activities. ■ Background checks on the Red Team members are conducted by the RT provider (as a minimum), including those required by the national authorities. ■ Multi-disciplinary composition of the Red Team, with a broad range of knowledge and skills, such as: business knowledge, red team testing, penetration testing, reconnaissance, threat intelligence, risk management, exploit development, physical penetration, social engineering, vulnerability analysis and combinations thereof. ■ Able to explain advanced, technical RT-subjects to both technical personnel (such as the members of the BT) and to non-experts in an understandable manner, guiding the CT through the RT phase in a clear manner. ■ Basic understanding of key financial processes, critical systems such as payment and settlement platforms, sector-specific challenges, and common cyber threats impacting the financial sector.
Technical requirements	■ Ability to deliver selected RT variant: – Assumed Compromise (minimum) – End-to-End Simulation – Scenario X (optional advanced/emerging threat scenario) ■ Use of MITRE ATT&CK or equivalent frameworks. ■ Clear rules of engagement and ethical boundaries.
Deliverables	■ Capability to produce a: – Red Team Test Plan (RTTP) detailing attack phases, TTPs, and risk controls. – Red Team Test Report (RTTR) summarizing actions, findings, and recommendations. ■ Ability to adapt scenarios dynamically during execution.
Security and governance	■ Demonstrable ISMS or equivalent security framework. ■ Secure handling and destruction of sensitive data post-test. ■ Compliance with GDPR and ART confidentiality protocols. ■ Ability to demonstrate risk management measures during testing.

7.3 Gold Team Provider Requirements

7.3.1 General requirements

Category	Requirements
Organisational requirements	■ Demonstrably relevant portfolio of comparable (preferably cyber) Crisis Management exercise assignments with at least three references from Crisis Management exercise engagements. ■ Capacity to form a Gold Team team of at least two persons, with additional capacity available if needed for tabletop or simulation forms. ■ Able to translate Red Team results into crisis management scenarios. ■ Has risk management and quality assurance capabilities for exercises. ■ Adequate indemnity insurance in place to cover activities which were not agreed upon in the contract and/or which stem from misconduct, negligence, etc. ■ No previous or current services delivered for the entity, that would present a conflict of interest for the Service Provider when conducting an ART test.
Team requirements	**Gold Team Lead** ■ Sufficient experience in Gold Teaming/Crisis Management exercises. At least 1 year of experience with managing (preferably Cyber) Crisis Management Exercises. ■ Up-to-date CV to be provided to the entity, specifically in delivering Gold Teaming/Crisis Management exercise activities. ■ Background checks on the Gold Team Lead are conducted by the Gold Teaming provider (as a minimum), including those required by the national authorities. ■ Able to translate advanced, technical RT subjects to organizational effects and explain technical subjects to non-technical personnel (such as the members of the board) and to non-experts in an understandable manner, guiding the CT through the GT phase in a clear manner. ■ Understands core financial processes, critical systems (such as payment and settlement platforms), sector-specific regulations and challenges, and common cyber threat scenarios affecting the financial sector. ■ Extensive project management capabilities, including the ability to organise its activities effectively, coordinate with relevant stakeholders, and deliver its contributions within agreed timelines and parameters. ■ Able to guide the Control Team (CT) throughout the GT phase in a structured and controlled manner.

Category	Requirements
Technical requirements	■ Ability to deliver selected GT variant: – Walk-through Session – Tabletop Exercise – Simulation (with or without counterplay). ■ Ability to develop GT scenarios based on relevant TI context, RT attack paths, observed control weaknesses and demonstrated business impact. ■ Capability to produce Master Scenario Event List (MSEL) with injects and scripts for TTX and SIM.
Deliverables	■ Gold team test plan (GTTP) including scope, learning goals, risk management measures, and a description of how TI context and RT findings are translated into GT objectives, injects and evaluation criteria. ■ Organization and execution of Gold Teaming Exercise. ■ Evaluation output: – Walkthrough: Action list – Tabletop: Observation report – Simulation: Full evaluation report with lessons learned.
Security and governance	■ Demonstrable ISMS or equivalent security framework. ■ Demonstrable containment measures to prevent leakage of scenario details. ■ Ability to ensure a safe learning environment for participants. ■ Compliance with confidentiality and GDPR requirements.

7.3.2 Walkthrough requirements

Category	Requirements
Facilitator/ observer	■ Able to lead and facilitate a discussion-based session. ■ Able to observe the session and identify improvement points. ■ The WS team must collectively cover knowledge of: – Project management – Crisis management and organisational resilience. ■ The WS team must collectively cover skills in: – Facilitation and session leading – Observation.

7.3.3 Tabletop requirements

Category	Requirements
Exercise Leader	■ Has demonstrable experience in running structured crisis-management exercises. ■ Is able to manage the overall flow of the TTX against the agreed learning goals, timeline and setup.
Facilitator	■ Has demonstrable experience in facilitating discussion-based crisis exercises. ■ Is able to guide the discussion through a storyline based on central dilemmas and injects. ■ Is able to present scenario information step-by-step and maintain the exercise format as a low-stress, discussion-based exercise.
Observer	■ Has demonstrable experience in observing participant behaviour and exercise outcomes in a crisis exercise setting. ■ Is able to capture observations against the learning goals. ■ Is able to support the hot-wash and identify immediate improvement points. ■ Is able to contribute to the observation report with actionable findings.

7.3.4 Simulation requirements

Category	Requirements
Exercise Leader	■ Has demonstrable experience in leading live crisis simulations. ■ Is able to coordinate the roles inside the exercise bubble and, where applicable, the response cell. ■ Is able to take overall responsibility for: – preparation – execution – evaluation of the SIM.
Facilitator/ trainer	■ Has demonstrable experience in facilitating high-pressure crisis simulations. ■ Is able to facilitate inside the exercise bubble and keep the simulation aligned with the scenario and learning goals. ■ Is able to support execution of a realistic, unfolding scenario using injects and/or simulated channels. ■ Has demonstrable experience in training participants during crisis simulations. ■ Is able to support participant learning during a real-time, stressful, unfolding scenario. ■ Is able to support the hot-wash and the training-oriented reflection after execution.
Observer	■ Has demonstrable experience in observing participant behaviour and exercise outcomes in a crisis exercise setting. ■ Is able to capture observations against the learning goals. ■ Is able to support the hot-wash and identify immediate improvement points. ■ Is able to contribute to the observation report with actionable findings.
Response cell (only in SIM B)	■ Has demonstrable experience in running counterplay / dynamic inject management in simulations. ■ Is able to generate and deliver dynamic responses based on participant decisions. ■ Is able to work with the response cell playbook and adjust injects within the agreed scenario boundaries. ■ Is able to support a realistic simulation without breaking control, confidentiality or learning goals.

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