|  |
| --- |
| ​ |
| [dd month yyyy] |
| ART Scoping Document [Code name test] |
|  |

Version management Format

|  |  |  |
| --- | --- | --- |
| **#** | **Date** | **Updated information** |
| 1.0 | May 2024 | Delivery ART Scoping Document Format, based on version 2.0 of the TIBER-NL Scoping Document Format |

Version management Scoping Document [Code name test]

|  |  |  |
| --- | --- | --- |
| **#** | **Date** | **Updated information** |
| [x.x] | [dd-mm-yyyy] | [version information] |
|  |  |  |
|  |  |  |
|  |  |  |

Table of contents

Table of contents 3

Format instructions 4

Format development and version updates 4

Purpose 4

Audience 4

Delivery process, responsibilities and approval 4

Terms of reference 5

Level of detail and pseudonymisation 5

Legal disclaimer and confidentiality 5

1. Document structure and required information 6

2. Executive Summary 8

3. Critical (sub)functions and justification 9

3.1 Introduction 9

3.2 Identification of critical functions and subfunctions 9

3.3 Systems and services to support the critical (sub)functions 9

4. Setting the flags 11

4.1 Flags 11

Format instructions

Format development and version updates

The Test Cyber Team (TCT) from De Nederlandsche Bank (DNB) has developed this Scoping Document format based on the TIBER-NL Scoping Document. This format will be periodically updated by the TCT-NL with the latest insights and feedback from the users of this document.

This chapter provides background information on why and how to use this ART Scoping Document format. All text that needs to be provided by the entity in order to complete this document, is indicated with […]. Once chapters 2 to 4 have been completed, the pages describing the ‘Format instructions’ can be deleted, for they are only intended to give guidance on the information to be shared.

This format is dated May 2024 (version 1.0).

Purpose

The purpose of the ART Scoping Document is to serve as:

* a comprehensive overview of the attack landscape of the entity, comprising of a complete overview of all its critical functions, subfunctions, key systems and services, and the ‘crown jewels’ (flags);
* a starting point for the Threat Intelligence Provider to gain understanding of the critical functions of this entity in order to perform the Targeted Threat Intelligence;
* a starting point - together with the outcomes of the Targeted Threat Intelligence – for the Red Team Provider to propose the most suitable test scenario’s in order to capture the defined flags during the test phase;

Audience

The ART Scoping Document is primarily aimed at providing an overview of the attack landscape of the entity for:

* the stakeholders on strategical/tactical level in the entity undertaking the ART test (eg. the Control Team, CISO, CIO, Board members of the entity);
* the Threat Intelligence Provider (TIP), the Red Team Provider (RTP) and/or the Gold Team Provider (GTP);
* the TCT (Test Manager (TM) and Threat Intelligence Manager (TI)) involved in the ART test;
* the entity’s supervision authority.

Delivery process, responsibilities and approval

The ART Scoping Document summarizes the outcomes of the scoping process in which the Control Team Lead (CTL) – possibly together with business experts – describes the critical functions of the entity. Critical functions are defined as the people, processes and technologies required to deliver a core service which, if disrupted, could have an impact on het Dutch financial stability, the entity’s safety and soundness, the entity’s customer base or its market conduct.

The Control Team Lead (CTL) is responsible for providing the Scoping Document as an outcome of the Engagement & Scoping steps in the preparation phase.

The Scoping Document has to be approved by the Control Team (CT) and C-level of the Entity and by the TCT during the scoping meeting.

Terms of reference

The ART Framework mandates that the scope of the test must include critical functions and their subsequent flags. The entity may expand the scope of the test beyond the critical functions to include other functions, if deemed appropriate. The CT should discuss the flags with the TM, who must approve them. Although the flags are set during the scoping process, they may be changed in some cases, based on threat intelligence and as the test evolves.

Level of detail and pseudonymisation

This format aims to provide a standardised approach and structure for the ART Scoping Document to entities undertaking an ART test.

The information in this Test Summary should be drafted in wording that is accessible to senior management. It should not contain names or detailed technical information that can reveal the identity of the entity. As is the rest of the documentation regarding the entity and the test, the information should be pseudonymized as much as possible (e.g. using the code name for the test).

Legal disclaimer and confidentiality

The information and opinions expressed in this document are for information purposes only. They are not intended to constitute legal or other professional advice.

All ART parties should use the Traffic Light Protocol when exchanging information (<https://www.us-cert.gov/tlp>).

1. Document structure and required information

The ART Scoping Document consists of the following chapters:

**Chapter 2 Executive summary**

This chapter provides a very high level overview of the critical functions and key systems and services of the organisation. The information presented in this chapter will be a summary of the more detailed information in the rest of the document.

**Chapter 3 Critical functions, key systems and justification**

ART follows the methodology as used in TIBER-NL and TIBER-EU to identify the attack landscape of the entity. This is done by cascading down from the critical functions of the entity to all possible individual flags and the target objectives to possibly be compromised during the test phase.

To make this practically workable, chapter 2 first provides an overview of the critical functions and their subfunctions. The critical functions can be derived from the potential critical functions for the entity’s sector as described in the current Generic Threat Landscape (GTL) as defined by TCT-NL. This chapter also presents all key systems and services and the justification of how and/or why these are used to support these critical (sub)functions. These steps are visualized in this picture and correspond with the actions number 1 and 2.



Following the TIBER-EU Framework, ART defines Critical Functions as *“the people, processes and technologies required by the entity to deliver a core service which, if disrupted, could have a detrimental impact on financial stability, the entity’s safety and soundness, the entity’s customer base or the entity’s market conduct”.*

The critical (sub)functions could be considered critical or essential to the financial services sector and/or a financial services sector organisation. Entities across the sector support and deliver these functions in different ways via their own internal processes, which are in turn underpinned by technological systems.

In some cases, these might also include the systems, people and business processes underpinning the entity’s critical functions that are outsourced to third-party service providers.

**Chapter 4 Setting the flags**

Based on the justification of defining which key systems and services are essential for providing the support to the critical functions of the entity, all possible crown jewels (flags) will be described this chapter. This detailing corresponds with number 3 is the picture above. Per flag will be defined what category of compromise (Confidentiality, Integrity and/or Availability) will cause a threat to the critical functions and what testing activity will demonstrate that compromise.

The information in this chapter will later on in the process - together with the outcomes of the Targeted Threat Intelligence – form the basis of the definition of the test scenario’s in the Red Team Testplan.

1. Executive Summary

This document presents an overview of the attack landscape of [CODE NAME] as a starting point for performing an ART test. It has been agreed by the TCT-NL and [CODE NAME].

Based on the views of all parties, the *critical functions* of [CODE NAME] are the following:

* [Please list the identified critical functions here]

The key systems and services that underpin each of the defined critical functions are:

* [Please list the identified key systems and services here]

For each system or service in scope a set of flags have been defined based on the primary risks to the business that could arise through the compromise of these systems or services. Threats to the information held on each system or service come under one of three categories, namely confidentiality, integrity and availability.

This document – together with the outcomes of the Targeted Threat Intelligence steps – will define what test scenario’s the Red Team Provider proposes to be most realistic for [CODE NAME]. The execution of the most realistic test scenario’s will provide the best learning experience when trying to compromise the confidentiality, integrity and/or availability of the flags in the key systems or services.

1. Critical (sub)functions and justification
	1. Introduction

This chapter provides an overview of the critical functions of [CODE NAME] and their sub-categories. It also provides insight in the underpinning key systems and services that deliver these critical functions. This chapter focuses on the description of the critical functions from a functional perspective and therefor describes what functions and supporting systems and services are crucial to [CODE NAME] for the core business.

* 1. Identification of critical functions and subfunctions

During the identification of the scope of the attack landscape, the focus was on those functions of the entity's business identified as presenting potential systemic risk to the financial stability of the financial system and/or the economy of the jurisdiction(s). For [CODE NAME] the following critical functions and sub-categories are identified:

* [Critical function 1 – subfunction(s) to support this critical function]
* [Critical function 2 – subfunction(s) to support this critical function]
* [Critical function 3 – subfunction(s) to support this critical function]
	1. Systems and services to support the critical (sub)functions

This paragraph presents all systems and services that are used to support the critical functions and their subfunctions. Per system/service the justification of how and/or why these are used to support these critical (sub)functions. Also the jurisdiction in which this system is hosted is provided.

| CRITICAL FUNCTION 1 |
| --- |
| SUBFUNCTION/-CATEGORY | JUSTIFICATION FOR INCLUSION OF CRITICAL FUNCTION AND SUBFUNCTION/-CATEGORY | SUPPORTING SYSTEMS/ SERVICES | SYSTEM/SERVICE PRESENT IN JURISDICTION |
| SUBFUNCTION A |  | SYSTEM 1 |  |
| SYSTEM 2 |  |
| SYSTEM 3 |  |
| SUBFUNCTION B |  | SYSTEM 2 |  |
| SYSTEM 4 |  |
| SYSTEM 5 |  |

| CRITICAL FUNCTION 2 |
| --- |
| SUBFUNCTION/-CATEGORY | JUSTIFICATION FOR INCLUSION OF CRITICAL FUNCTION AND SUBFUNCTION/-CATEGORY | SUPPORTING SYSTEMS/ SERVICES | SYSTEM/SERVICE PRESENT IN JURISDICTION |
| SUBFUNCTION C |  | SYSTEM 6 |  |
| SYSTEM 2 |  |
| SYSTEM 7 |  |
| SUBFUNCTION D |  | SYSTEM 7 |  |
| SYSTEM 8 |  |
| SYSTEM 9 |  |

| CRITICAL FUNCTION 3 |
| --- |
| SUBFUNCTION/-CATEGORY | JUSTIFICATION FOR INCLUSION OF CRITICAL FUNCTION AND SUBFUNCTION/-CATEGORY | SUPPORTING SYSTEMS/ SERVICES | SYSTEM/SERVICE PRESENT IN JURISDICTION |
| SUBFUNCTION E |  | SYSTEM 10 |  |
| SYSTEM 2 |  |
| SYSTEM 6 |  |
| SUBFUNCTION F |  | SYSTEM 3 |  |
| SYSTEM 4 |  |
| SYSTEM 5 |  |

1. Setting the flags

This chapter provides the connection between the already provided overview of the key systems and services that deliver the critical functions and their subfunctions and the possible flags/the so-called ‘crown jewels’ within these key systems when compromised. The information in this chapter will later on in the process - together with the outcomes of the Targeted Threat Intelligence – form the basis of the definition of the test scenario’s in the Red Team Testplan.

* 1. Flags

Based on the justification of defining which key systems and services are essential for providing the support to the critical functions of the entity, all possible crown jewels (flags) will be described this paragraph. This detailing corresponds with number 3 is the picture in chapter 1. Per flag will be defined what category of compromise (Confidentiality, Integrity and/or Availability) will cause a threat to the critical functions and what testing activity will demonstrate that compromise.

|  |
| --- |
| CRITICAL FUNCTION 1 – SUBFUNCTION A |
| SUPPORTING SYSTEM/SERVICE | JUSTIFICATION FOR INCLUSION SYSTEM/SERVICE AND SUPPORT TO CRITICAL (SUB)FUNCTION | INFORMATION ASSURANCE THREAT CATEGORY (C, I, A) | FLAG/OBJECTIVE TO DEMONSTRATE COMPROMISE C, I OR A OF SYSTEM |
| SYSTEM 1 |  |  |  |
| SYSTEM 2 |  |  |  |
| SYSTEM 3 |  |  |  |

|  |
| --- |
| CRITICAL FUNCTION 1 – SUBFUNCTION B |
| SUPPORTING SYSTEM/SERVICE | SYSTEM/SERVICE PRESENT IN JURISDICTION | INFORMATION ASSURANCE THREAT CATEGORY (C, I, A) | FLAG/OBJECTIVE TO DEMONSTRATE COMPROMISE C, I OR A OF SYSTEM |
| SYSTEM 2 |  |  |  |
| SYSTEM 4 |  |  |  |
| SYSTEM 5 |  |  |  |

|  |
| --- |
| CRITICAL FUNCTION 2 – SUBFUNCTION C |
| SUPPORTING SYSTEM/SERVICE | SYSTEM/SERVICE PRESENT IN JURISDICTION | INFORMATION ASSURANCE THREAT CATEGORY (C, I, A) | FLAG/OBJECTIVE TO DEMONSTRATE COMPROMISE C, I OR A OF SYSTEM |
| SYSTEM 6 |  |  |  |
| SYSTEM 2 |  |  |  |
| SYSTEM 7 |  |  |  |