NORGES BANK

-TIBER-NO
Scope Specification template

Version 1.3, October 2023

Contents

How to use this document

This document is a template and has the scope elements the Entity should specify. Guidance for this process can be found at the end of the document in 5 Scoping guidance. The guidance should be used together with this template to make a specific Scope Specification document containing the specific scope for the test. In this template, text marked with yellow should be replaced with test specific information.

Executive summary

This document presents the detailed scope for the TIBER-NO test with the code name CODE NAME. The content has been agreed by TCT-NO and the TCT(s) in JURISDICTION(s) XX.

Based on the views of all parties, the **critical functions** to be included in the TIBER-NO scope are as follows:

- SUMMARISE CRITICAL FUNCTIONS HERE

The **key systems and services** that underpin each of the scoped critical functions are listed below:

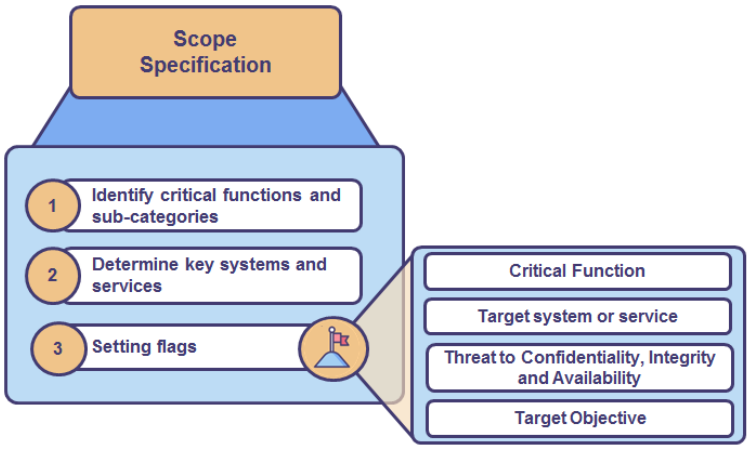
- LIST THE SYSTEMS/SERVICES HERE FOR EACH CRITICAL FUNCTION INCLUDED IN THE SCOPE HERE

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. These flags are summarized in a table in **Error! Reference source not found. Error! Reference source not found.**.

Threats to the information held on each system or service come under one of three categories, namely confidentiality, integrity, and availability. The action undertaken by Red Team provider to prove compromise will be dependent on which of the three categories each service or system falls within.

1 Introduction

This document describes in detail the scope for testing following TIBER-NO for CODE NAME. The content is agreed between TCT and the Entity. The document is based on «TIBER-EU Scope Specification Template» and details the specific areas for this test and should be used as a reference when working with this document. The following figure visualizes the most important components of the scope specification.



2 Critical functions

This section presents the critical functions of the Entity. The TIBER-EU Framework 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".

Code	Function	CIA	Included because

3 Key systems and services

This section presents a description of the key systems and services (processes and/or people/key roles) that underpin each critical function in scope for the TIBER-EU test.

Selected critical function	System/service supporting the function	Included because

4 Flags

This section presents a description of the flags to be achieved by the Red Team in the Red Team testing phase. Each flag is linked to a scenario and at least one flag must be defined per scenario.

This is a summarizing table of the defined flags.

#	Flag description	Scenario	CF	System	Phase

5 Scoping guidance

This section contains guidance for the scope specification.

5.1 Recommendations for naming convention

As TIBER tests consists of numerous components, TCT proposes using a standardized naming convention for all components. This is based on a system of codes per component, with letters and numbers as unique identifiers. These conventions are not derived from the TIBER-EU framework and are merely a suggestion by TCT-NO for increased consistency in TIBER-NO tests.

Flags and leg-ups are directly tied to scenarios. While leg-ups might be the same for multiple scenarios, they should be defined as separate leg-ups with individual codes linked to scenario with the letter of the scenario. Critical functions (CFs) and risks are independent of scenarios, thus there is nothing in the CF or risk codes indicating they belong to a specific scenario. Here is a table with examples of the recommended naming conventions:

Component	Code	Example
Critical functions	CF-[number]	CF-01
Scenarios	SC-[letter]	SC-A
Flags	FL-[scenario-letter]-[number]	FL-A-01 (for scenario A)
Leg-ups	LU-[scenario-letter]-[number]	LU-A-01 (for scenario A)
Risks	RI-[number]	RI-01

5.2 Critical functions

This section describes how to define the Critical functions for the test.

The TIBER-EU Framework 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".

Identifying the CFs involves using criteria for Critical Functions from the Single Resolution Board (SRB). However, the assessment of what constitute critical functions and the overall determination of the entities and functions to be tested are the responsibility of Finanstilsynet and Norges Bank via these fora. According to SRB, to be considered critical, a function needs to fulfil both of the following:

- (a) "the function is provided by an institution to third parties [which are] not affiliated to the institution or group; and
- (b) a sudden disruption would likely have a material negative impact on the third parties, give rise to contagion or undermine the general confidence of market participants due to the systemic relevance of the function for the third parties and the systemic relevance of the institution or group in providing the function".

Each CF should be named, given a code, indicating if its impact is on confidentiality, integrity and integrity, and why it is included. Note that a CF is *not* the same as a critical system or critical IT service, even though they are intrinsically linked.

Example of Critical Functions:

Code	Function [example]	CIA [example]	Included because [example]
CF-01	International payments	CIA	Key financial function with material negative impact to international third parties if compromised.
CF-02	IT service availability	A	The availability of the underlying IT services such as the central directory service (Active Directory) is essential to maintain financial services and losing it directly impacts financial stability.

5.3 Key systems and services

This section explains how to describe the key systems and services (processes and/or people/key roles) that underpin each critical function in scope for the TIBER-EU test.

A CF can be supported by multiple systems and services. Each key system must be associated with a CF and a reason must be provided for its inclusion in testing. Reasons for inclusion can be relevance to threat landscape, system criticality and supporting the selected CF.

Example of systems related to the CFs from Chapter 2 in this guide:

Selected critical function	System/service supporting the function	Included because
Internal payments (CF-01)	SWIFT	SWIFT is essential for payments to international third parties. A compromise of this system has significant negative impact for third parties and financial stability.
Availability of IT services (CF-02)	Active Directory	The central directory service is essential for the bank to continue its operations. Without access to this service, the bank does not function, and this directly impacts the bank's IT service availability which is defined as a critical function.

5.4 Flags

This section presents how flags to be achieved by the Red Team in the Red Team testing phase can be described. Each flag is linked to a scenario and at least one flag must be

defined per scenario. This is an example of a table of the defined flags for the previous CFs and systems.

#	Flag description	Scenario	CF	System	Phase
FL-A-01	Initiate transfer of 1 MNOK	SC-A	CF-01	SWIFT	OUT
FL-B-01	Demonstrate sufficient access to perform ransomware operation.	SC-B	CF-02	AD	OUT

There are often multiples flags per scenario in a TIBER test. Once all scenarios are defined, it can be a good idea to make a table to summarize the flags for all scenarios and indicate which phase they are relevant for. A pitfall of this process is to make too many flags, which can lead to the Red Team being distracted by an attempt to capture all the flags. TCT-NO therefore recommends few flags, and that they mainly align with the threat actor goals for each scenario.

Annex 1 - Change log

Version	Date	Change
1.3	17.10.2023	Guidance moved to end of document.
1.2	10.05.2023	New naming convention guidance and flag design with examples.
1.1	16.03.2023	Changed language to English and moved to NB word template.
1.0	xx.xx.2023	Initial version