NORGES BANK

TIBER-NO
Scope specification template

Version 1.2, May 2023

TLP:AMBER

Contents

How to use this document

This document contains three components:

- Content and guidance from the TIBER-EU Scope Specification Template
- Guidance from TCT for defining the scope of a TIBER test, including examples
- The scope elements the Entity should specify themselves

This document may be used to make a specific version containing only the scope for the test without the supporting guidance and examples:

- Text marked with yellow should be replaced with test specific information
- Text and examples marked with a light gray color are guidance and can safely be removed. The Entity can choose to keep whatever guidance they like in the final document for future reference.

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:

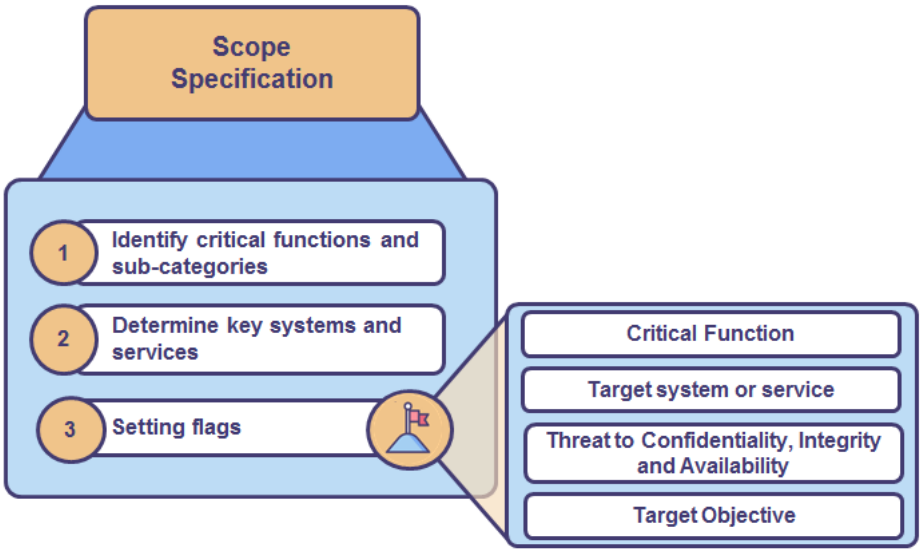
- LIST THE SYSTEMS/SERVICES HERE FOR EACH CRITICAL FUNCTION INCLUDED IN THE SCOPE HERE

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 4.1 Flag summary.

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 CODENAME. 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.



1.1 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 is 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

2 Critical functions

This section presents the critical functions of the entity.

Code	Function	CIA	Included because

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, indicated 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.

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

Only the key systems and services need to be included in the list below.

A CF can be supported by multiple systems and services. Each key system must be associated to a CF, described 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:

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.

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.

Flag: FL-[scenario-code]-[number]: Name of flag	
Critical function	
Target system or service	

Information Assurance threat category (Confidentiality, Integrity, Availability)	
Description of system/service function	
Objective - i.e., testing activity or technique required to demonstrate compromise	
Goal – What is the threat actor trying to achieve? This can refer to Mitre Tactic if applicable.	
Phase (IN, THROUGH, OUT)	

The flags should be designed so they encompass all three major test phases: IN, THROUGH and OUT. There should be at least one flag for each phase, and ideally more than one for the OUT phase, which is the final goal for the threat actor, e.g., stealing money or distribute ransomware. The flags are subject to change based on the Targeted Threat Intelligence and red team test phases of the TIBER test.

Example of a flag:

[Example] Flag: FL-B-02: Read access to settlement information	
Critical function	CF-01 – Settlement bank
Target System or Service	Payment System Name
Information Assurance threat category (Confidentiality, Integrity, Availability)	C-I-A
Description of system/service function	SWIFT ensures national bank settlements which is critical for national financial stability.
Objective - i.e., testing activity or technique required to demonstrate compromise	Screenshots or log entries demonstrating access to settlement information.
Goal – What is the threat actor trying to achieve? This can refer to Mitre Tactic if applicable.	Sell this information to third parties for profit.
Phase (IN, THROUGH, OUT)	OUT

Another example of a flag:

[Example] Flag: FL-A-01: Acquire Domain Admin rights	
Critical function	Availability of critical IT services
Target System or Service	Active Directory Domain Services
Information Assurance threat category (Confidentiality, Integrity, Availability)	C-I-A

Description of system/service function	Central identity management system, critical for managing access to all services in the entity.
Objective - i.e., testing activity or technique required to demonstrate compromise	Screenshots or log entries demonstrating Domain Admin rights, for example by performing tasks only a member of the Domain Admins group can perform such as logging in to a domain controller.
Goal – What is the threat actor trying to achieve? This can refer to Mitre Tactic if applicable.	Privilege Escalation – Acquire sufficient privileges and persistence access to facilitate the OUT phase.
Phase (IN, THROUGH, OUT)	THROUGH

4.1 Flag summary

This is a summarizing table of all the flags.

CF	System	Phase	Flag

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.

This is an example of such a table:

CF	System	Phase	Flag
Availability of IT services	Active Directory	IN	FL-A-01: Establish a foothold in the organisation
		THROUGH	FL-A-02: Gain access to Domain Admin rights.
		OUT	FL-A-03: Demonstrate sufficient access to perform ransomware operation.
		OUT	FL-A-04: Exfiltration of sensitive banking information
Settlement Bank	ExampleCorp	IN	FL-B-01: Establish a foothold in the organisation
		IN	FL-B-02: Application-level access to the service
		THROUGH	FL-B-03: Gain code execution on servers hosting the service
		OUT	FL-B-04: Modify information in the service
		OUT	FL-B-05: Modify files being exchanged in the service
Business bank	ExampleBank	IN	FL-C-01: Application-level access to the service

		IN	FL-C-02: Gain code execution on web server hosting the service
		THROUGH	FL-C-03: Access to case worker user account
		THROUGH	FL-C-04: Read access to payment files
		OUT	FL-C-05: Exfiltration of payment files
		OUT	FL-C-06: Exfiltration of account information

Annex 1 - Change log

Version	Date	Change
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