EUROPEAN CENTRAL BANK

EUROSYSTEM

TIBER-EU

Scope Specification Document Guidance

January 2025

Contents

1 Introduction

The Scope Specification Document (SSD) summarizes the critical or important functions (CIF) of a financial entity as the basis for a TIBER test. As such, it provides the boundaries of the test and the list of options from which the relevant scenarios to be tested are chosen, based on the threat-landscape of the financial entity identified in the threat intelligence phase. It therefore serves as a starting point for the threat intelligence provider (TIP) to gain an understanding of the CIFs of this entity in order to perform the targeted threat intelligence. Additionally, the scope enables the test manager (TM) to review and provide feedback on scenario selection, ensuring the test focusses on systemically CIFs, thus enhancing their effectiveness and impact.

1.1 Purpose of this document

The purpose of this document is to provide the relevant stakeholders with information on the requirements[1] for the goal, content and format of a TIBER-EU SSD. It also aims at providing guidance on important aspects to be considered during drafting as well as supporting material.

1.2 Target audience

This TIBER-EU Scope Specification Document Guidance is mainly aimed at the control team (CT) creating a SSD during the preparation phase of a TIBER test. Beyond that, it is useful to read for all stakeholders of a TIBER engagement to understand the nature of its content.

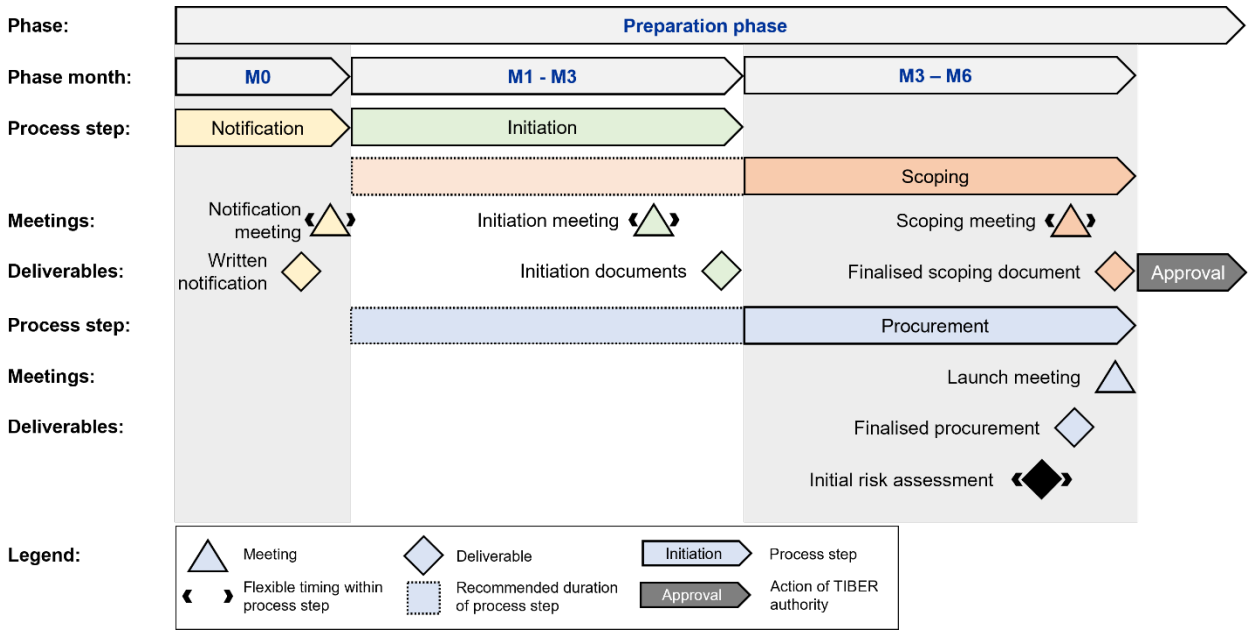
1.3 Location within testing process

The SSD is created during the scoping process step within the preparation phase of a TIBER Test. It summarizes the outcomes of the scoping process in which the CT – possibly together with business experts – describes all CIFs of the entity, as well as preliminary set of flags to be captured.

[1] In addition to the minimum requirements for complying with the TLPT obligations under DORA, this document also includes operational TIBER-EU guidance based on best practices, knowledge and experience from numerous previous tests.

Figure 1[2]

Preparing the Scope Specification Document



[2] Note that only the actions of the TIBER authority are included in the figure that have an impact on the timelines of the test. The figure is not an exhaustive overview of all actions to be undertaken by the involved stakeholders.

2 Required content of the Scope Specification Document

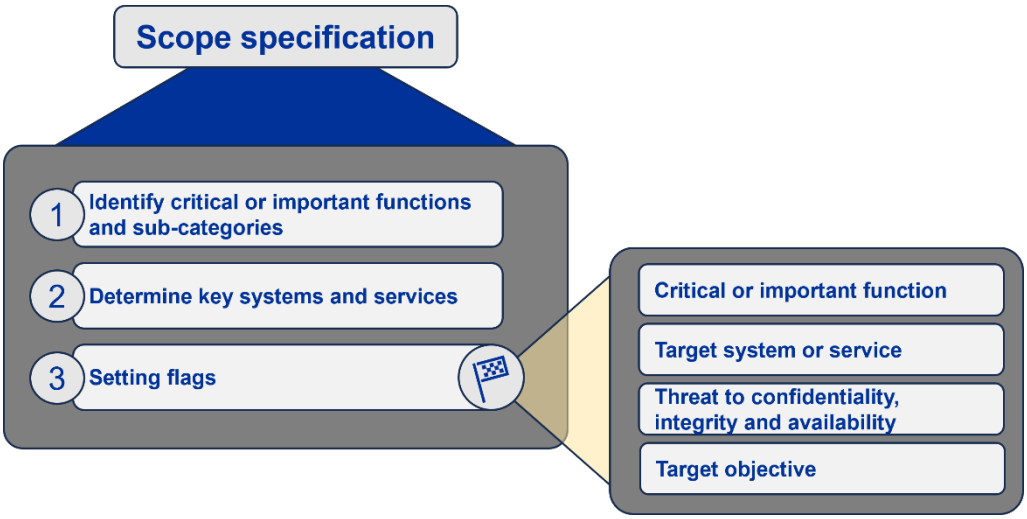
The SSD shall contain, at a minimum, the following elements:

- a list of all CIFs identified by the financial entity;
- for each identified CIF, the following information shall be included:
    - where the CIF is included in the scope of the test, the explanation of the reasons for its inclusion;
    - where the CIF is not included in the scope of the test, the explanation of the reasons for which it is not included;
- the identified ICT system(s) supporting this CIF;
- for each identified ICT system:
    - whether it is outsourced and if so, the name of the ICT third-party service provider;
    - the jurisdictions in which the ICT system is used;
- a high-level description of preliminary flag(s), indicating which security aspect of confidentiality, integrity, availability is covered by each flag.

3 Considerations when drafting the Scope Specification Document

The means of this document is to identify the attack surface of the entity. This is achieved by cascading down from all the CIFs of the entity to all possible individual flags and the target objectives to possibly be compromised during the test.

Figure 2
Defining the scope of the test



3.1 Critical or important functions

CIFs are defined as:

"*a function, the disruption of which would materially impair the financial performance of a financial entity, or the soundness or continuity of its services and activities, or the discontinued, defective or failed performance of that function would materially impair the continuing compliance of a financial entity with the conditions and obligations of its authorisation, or with its other obligations under applicable financial services law*"[3].

Disruption to these functions could lead to widespread consequences, including operational failures, reputational damage, regulatory penalties, and potential ripple effects

[3] As defined under DORA, article 3(22).

across the financial system, highlighting their importance to both the entity and the broader financial ecosystem.

The critical (sub)functions could be considered critical or important 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.

The TIBER-EU framework mandates that the SSD for the test must list all identified CIFs of the entity. When doing so, entities shall consider the following criteria for the inclusion of the CIFs in the scope of the test:

- the criticality or importance of the function and its possible impact to the financial sector and on financial stability at national and Union level;
- the importance of the function for the day-to-day business operations of the financial entity;
- the exchangeability of the function;
- the interconnectedness with other functions;
- the geographical location of the function;
- the sectoral dependence of other entities on the function;
- where available, threat intelligence concerning the function.

Where the CIF is not included in the scope of the test, an explanation will be provided of the reasons for which it is not included.

The entity may expand the scope of the test beyond the CIFs to include other functions, if deemed appropriate by the entity in consultation with the TM and as long as the inclusion does not negatively impact the test of the CIFs. It may be the case that some of the CIFs in scope are ultimately not tested, as the final scenarios will be determined by the outcome of the threat intelligence phase as described in the TIBER-EU Framework.

3.2 Critical systems

CIFs as well as their subfunctions are underpinned by critical systems, people and business processes. The entity shall present all critical systems and services including a justification of how and why these are used to support these critical (sub)functions. These steps are visualized in Figure 2 and correspond with the actions number 1 and 2.

In some cases, these critical systems and services might also include those that are supported by ICT third-party service providers.

3.3 Flags

Based on the justification of defining which critical systems and services are essential for providing the support to the CIFs of the entity, all possible flags are described in this chapter. This detailing corresponds with action number 3 in Figure 2. For each flag, the category of compromise (confidentiality, integrity, availability) that causes a threat to the CIFs shall be defined. Additionally, the flag details have to be included, explaining which testing activity demonstrates compromise, i.e. what has to happen for the flag to be considered to be reached.

Although the flags are set during the scoping process step, they can be changed on an iterative basis following the threat intelligence process results, Red Team Test Plan (RTTP) and on the basis of the active red team test progress.

The information in this chapter serves as foundational input for refinement in the construction and operationalisation of threat intelligence-based test scenarios by the TIP and red team testers (RTT).

4 Drafting format

The TIBER-EU Scope Specification Document may be drafted in any preferred format, provided that all required information is included. All content that needs to be provided in order to complete this document is indicated in chapter 2 of this document. Example templates to be used on a voluntary basis are provided in the annexes and might prove helpful for better formalisation.

5 Annex

5.1 Annex 1: Template for executive summary

This document presents an overview of the critical or important functions (CIF) and their supporting systems and services of [CODE NAME] as a starting point for performing a TIBER-[XX] test. It has been agreed by the TM(s) in jurisdiction(s) XX and [CODE NAME].

Based on the views of all parties, the CIFs of [CODE NAME] are the following:

[Please list the identified critical or important functions here]

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

[Please list the identified key systems and services here]

For each system or service in scope, a set of flags has been defined, based on the primary risks to the business that could arise through the compromise of these systems or services. Threats to each function, system or service are listed under confidentiality, integrity and/or availability.

This document serves as key input for the construction and operationalisation of the most relevant threat intelligence-based test scenarios by the TIP and RTT for [CODE NAME]. The execution of the most relevant test scenarios 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.

5.2 Annex 2: Template for critical or important functions, subfunctions and justification

The below suggested table provides an overview of the CIFs of [CODE NAME] and their subfunctions. It also provides insight in the underpinning systems and services that deliver these CIFs, including whether these are supported by ICT third-party providers (ICT TPP). The table focuses on the description of the CIFs from a functional perspective and therefor describes what functions and supporting systems and services are crucial to [CODE NAME] for the core business.

Functions of the entity's business identified as representing potential systemic risk to the stability of the financial system and/or the economy of the jurisdiction(s) are in focus during the identification of the scope. For [CODE NAME] the following CIFs and subfunction(s) are identified:

[CIF 1 – subfunction(s) to support this CIF]

[CIF 2 – subfunction(s) to support this CIF]

[CIF 3 – subfunction(s) to support this CIF]

[…]

CRITICAL OR IMPORTANT FUNCTION [1]				
SUBFUNCTION	JUSTIFICATION FOR INCLUSION OF CIF AND SUBFUNCTION	SUPPORTING SYSTEMS/ SERVICES	SYSTEM/SERVICE USED IN JURISDICTION	SYSTEM/SERVICE supported by ICT TPP
[SUBFUNCTION A]		[SYSTEM 1]		
		[SYSTEM 2]		
		[SYSTEM 3]		
[SUBFUNCTION B]		[SYSTEM 2]		
		[SYSTEM 4]		
		[SYSTEM 5]		

CRITICAL OR IMPORTANT FUNCTION [2]				
SUBFUNCTION	JUSTIFICATION FOR INCLUSION OF CIF AND SUBFUNCTION	SUPPORTING SYSTEMS/ SERVICES	SYSTEM/SERVICE USED IN JURISDICTION	SYSTEM/SERVICE supported by ICT TPP
[SUBFUNCTION C]		[SYSTEM 6]		
		[SYSTEM 2]		
		[SYSTEM 7]		
[SUBFUNCTION D]		[SYSTEM 7]		
		[SYSTEM 8]		
		[SYSTEM 9]		

EXAMPLE: CRITICAL OR IMPORTANT FUNCTION: INTERBANK PAYMENTS				
SUBFUNCTION	JUSTIFICATION FOR INCLUSION OF CIF AND SUBFUNCTION	SUPPORTING SYSTEMS/ SERVICES	SYSTEM/SERVICE USED IN JURISDICTION	SYSTEM/SERVICE SUPPORTED BY ICT TPP
Payment Services to MFIs	*Payment services to major financial institutions (MFIs) are critical for financial stability. MFIs, as key players in the global economy, rely on seamless interbank payments to maintain liquidity, manage risks, and ensure operational resilience. Facilitating these payments prevents liquidity crises, maintains market confidence, and promotes efficient capital markets, essential for overall financial stability.*	*SWIFT network infrastructure*	*Two-letter country code as defined in ISO 3166*	*SWIFT*
		SWIFT gateway & web access	*Two-letter country code as defined in ISO 3166*	SWIFT
Clearing House Operations	*Clearing house operations play a critical role in ensuring the efficient and orderly settlement of financial transactions. By providing central counterparty services, clearing houses mitigate counterparty risk, reduce settlement risk, and promote confidence in financial markets.*	*Clearing system A*	*Two-letter country code as defined in ISO 3166*	*n/a*
		Clearing system B	*Two-letter country code as defined in ISO 3166*	*n/a*

5.3 Annex 3: Template for setting the flags

The table below provides the connection between the already provided overview of the key systems and services that deliver the CIFs, their subfunctions, and the possible flags within these key systems when compromised. The information in this table serves as foundational input for refinement in the construction and operationalisation of threat intelligence-based test scenarios by the TIP and RTT.

Based on the justification of defining which key systems and services are essential for providing the support to the CIFs of the entity, all possible flags could be described in the following form. This detailing corresponds with action number 3 figure 1. Per flag is defined what category of compromise (Confidentiality, Integrity and/or Availability) will cause a threat to the CIF and what testing activity will demonstrate that compromise.

CRITICAL OR IMPORTANT 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 OR IMPORTANT FUNCTION [1] – [SUBFUNCTION B]			
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 2]			
[SYSTEM 4]			
[SYSTEM 5]			

CRITICAL OR IMPORTANT FUNCTION [2] – [SUBFUNCTION C]			
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 6]			
[SYSTEM 2]			
[SYSTEM 7]			

EXAMPLE: CRITICAL OR IMPORTANT FUNCTION: INTERBANK PAYMENTS – SUBFUNCTION: PAYMENT SERVICES TO MFI'S			
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
SWIFT network infrastructure	"*The SWIFT Network Infrastructure connects thousands of financial institutions globally, providing a secure, reliable, and standardized platform for exchanging payment messages. It ensures seamless global connectivity, safeguarding transactions through encryption and secure messaging protocols, and reduces the risk of errors through standardized message formats, which are crucial for efficient and consistent interbank payments.*"	Availability	Demonstrate the ability to disrupt the internal SWIFT infrastructure, causing delays or outages in financial transactions.
SWIFT gateway & web access	"*The SWIFT Gateway and Web Access allow institutions to securely access the SWIFT network for sending and receiving financial messages. The gateway provides a secure entry point, while web access enhances flexibility by allowing institutions to manage transactions remotely. These tools ensure controlled, authenticated access to the network, facilitating efficient, secure interbank payments.*"	Integrity	Demonstrate the theft of funds by changing the accounts receivable.

Postal address 60640 Frankfurt am Main, Germany
Telephone +49 69 1344 0
Website www.ecb.europa.eu

For specific terminology please refer to the ECB glossary (available in English only).

PDF ISBN 987-xx-xxx-xxxx-x, ISSN xxxx-xxxx, doi:xx.xxxx/xxxxxx, QB-xx-xx-xxx-EN-N
HTML ISBN 987-xx-xxx-xxxx-x, ISSN xxxx-xxxx, doi:xx.xxxx/xxxxxx, QB-xx-xx-xxx-EN-Q