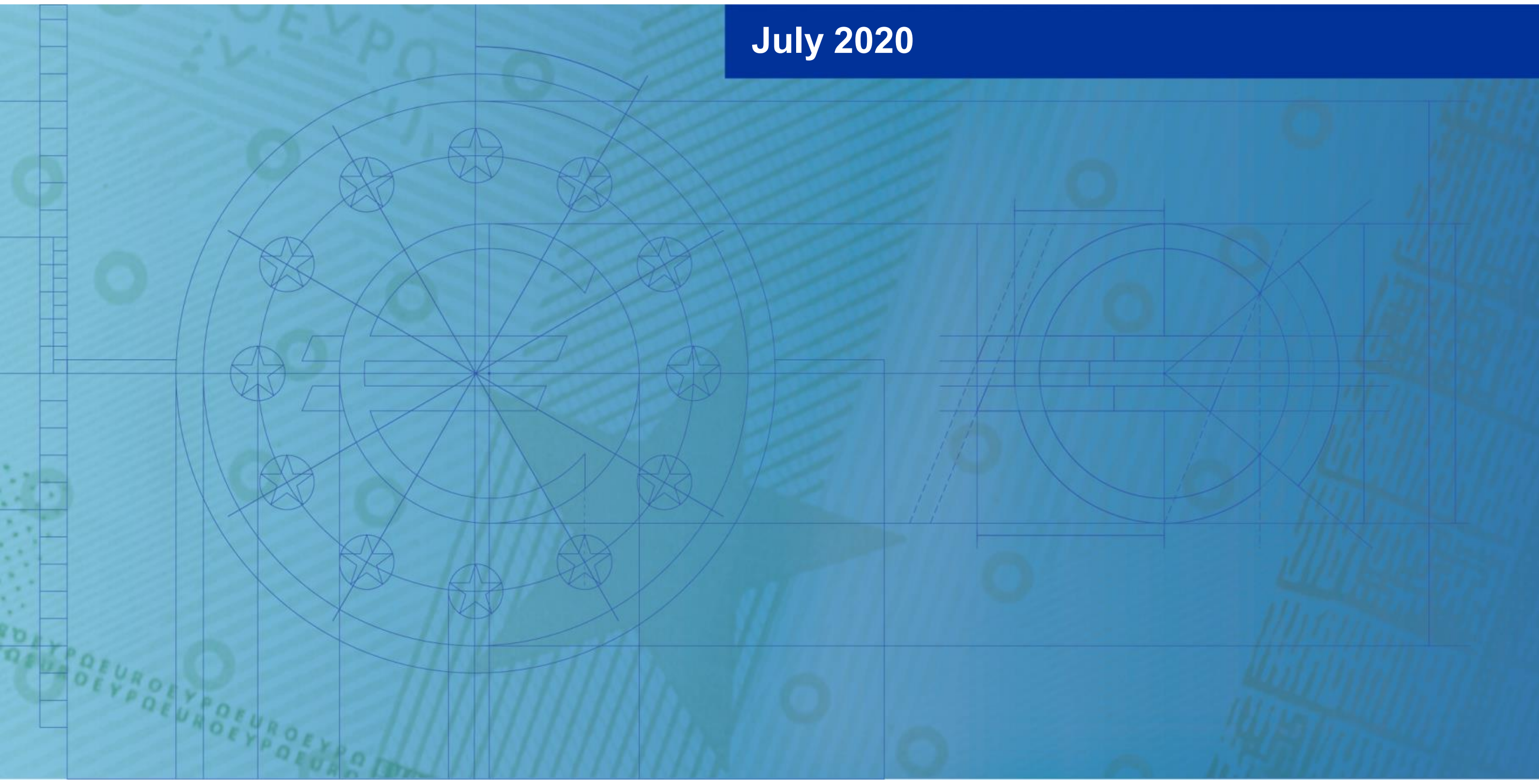
EUROPEAN CENTRAL BANK
EUROSYSTEM

TIBER-EU

Scope Specification Template

CHANGE LOG

Version	Date	Comments



July 2020

Contents

1 Executive Summary

This document presents the detailed scope for the [NAME OF ENTITY/ CODE NAME] TIBER-XX test. It has been agreed by the TCT(s) in JURISDICTION(s) XX and [NAME OF ENTITY/CODE NAME].

Based on the views of all parties, the **critical functions** of [NAME OF ENTITY's/CODE NAME] business to be included in the TIBER-XX scope are as follows:

[SUMMARISE CRITICAL FUNCTIONS HERE]

The **key systems and services** that underpin each of the scoped critical functions are summarised 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.

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.

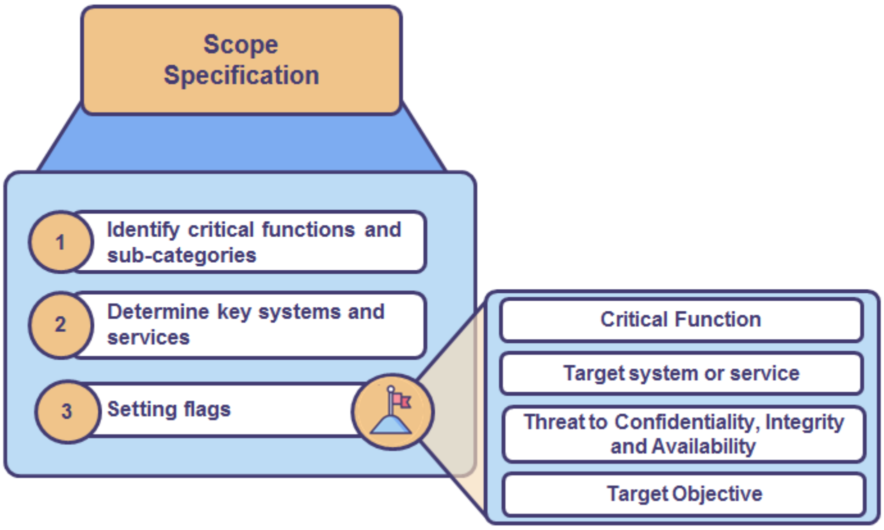
2 Introduction

2.1 Purpose of this document

This template is to be used during any TIBER-EU test by the tested entity to present the detailed scope of its respective test. The scope has to be agreed by the tested entity at board level and by the TIBER Cyber Teams (TCTs) of the involved authorities. For more detail please consult the TIBER-EU Framework[1] and related TIBER documentation.

This template aims to standardise the scoping phase of the TIBER-EU testing process amongst financial entities and TCTs, to ensure that TIBER-EU is implemented in a harmonised manner and to facilitate the mutual recognition of test results.

The overall methodology for scoping is to identify the critical functions and sub-categories of the entity; identify the underpinning key systems and services that deliver the critical functions; and to set the flags for the test, that will test the confidentiality, integrity and/or availability of the entity's critical functions and systems and services.


Scope Specification
1 Identify critical functions and sub-categories
2 Determine key systems and services
3 Setting flags
Critical Function
Target system or service
Threat to Confidentiality, Integrity and Availability
Target Objective

2.2 Terms of reference

The TIBER-EU Framework mandates that the scope of the test must include critical functions, and the entity may expand the scope of the test beyond the critical functions to include other functions, if deemed appropriate. Following the threat intelligence phase, it may be the case that some of the critical functions are not

[1] https://www.ecb.europa.eu/pub/pdf/other/ecb.tiber_eu_framework.en.pdf

tested, as the final scope will be determined by the threat intelligence. 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”.

Note that a critical function is not a system. It is a function which 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. It is these technological systems, processes, and the people surrounding them that are the focus of the threat intelligence and red team testing phases. In some cases, this will also include the systems, people and business processes underpinning the entity’s critical functions that are outsourced to third-party service providers.

When defining the scope of the TIBER test, consideration has therefore primarily been given to 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).

Testing must be performed on the live production systems of the entity. However, the entity may also include other types of systems, including shared IT platforms and services as well as pre-production, testing, backup and recovery systems, within the scope of the red team test.

This TIBER-EU Scope Specification template allows the entity to set out the scope of the TIBER-EU test, and lists the key systems and services that underpin each critical function. This information helps the entity set the “flags” to be captured, which are essentially the targets and objectives that the red team (RT) providers must strive to achieve during the test, using a variety of tactics, techniques and procedures (TTPs). These targets and objectives aim to structure the approach of the RT provider, to explore whether they are successfully capable of compromising the Confidentiality, Integrity and/or Availability of the system, service or information held therein.

Consistent with the main international standards on information security, threats to the information held on each system or service come under one of three categories, namely Confidentiality, Integrity and Availability. The actions undertaken by RT providers to prove compromise will be dependent on which of the three categories each service or system falls within.

As a result of producing this document, all involved parties (TCTs of the involved authorities, White Team (WT), the Board of the entity, the threat intelligence (TI) and red team (RT) providers) will gain a detailed understanding of the overall scope of the entity for the TIBER-EU test. This document will also help the TI provider to focus its targeted threat intelligence activities in order to provide the RT provider with the requisite information to help capture the flags during the red team test.

Due to the sensitive nature of the information it contains, this document, once complete, should be handled and treated as highly confidential and stored in a manner commensurate with this classification (e.g. TLP Amber).

2.3 Structure of this document

The remainder of this document is structured as follows:

- Section 2, Critical Functions, presents the critical functions of the entity;
- Section 3, Key systems and services, presents a description of the key systems and services that underpin each critical function;
- Section 4, Setting the Flags, presents compromise targets and objectives for each system or service in scope.

3 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".

For example, amongst others, some critical functions could be: (i) deposit taking and savings; (ii) lending and loan servicing; (iii) capital markets and investment; (iv) wholesale funding markets; and (v) payments, clearing, custody and settlement.[2]

Entities should have an information security/cybersecurity framework in place, and a key component of this is the *Identification* process. The Identification process requires an entity to identify and document all its critical functions, technological systems, processes and the people that support those functions, and update this information on a regular basis. During the Scoping process, it is recommended that entities use the information from the Identification process, to set out their critical functions, which should be in scope of the TIBER test. **It is critical that the entity identifies critical functions that are outsourced and cite to whom these are outsourced.**

Some entities may provide several critical functions as part of their business model, and each of these critical functions may have sub-categories of functions. For example, an entity that provides *clearing and settlement* may break this function down further, into a number of sub-categories. For example:

Critical Function	Sub-categories	Justification for inclusion
Deposit taking and savings	Current accounts	
	Savings accounts	
	Retail internet banking	
	Debit cards	
	ATM cards	
	Credit cards	
	Mortgages	
	Home equity loans	

[2] See for examples of and further elaboration on critical functions e.g. "Guidance on Identification of Critical Functions and Critical Shared Services" (FSB, 2013) and "Critical Functions: SRB Approach" (SRB, 2017), which however are geared towards banks only. For FMIs, there is no reference document as such available; the Principles for Financial Market Infrastructures (CPMI, 2012) mention "critical operations and services" without providing further examples.

	Personal loans	Deposit taking and savings services are a core function for the real economy, and any disruption to these would have a detrimental impact on the customer base. Customers of a disrupted deposit taker may lose immediate access to their deposits, and thus are not able to execute payments. In the event of disruption to a significant deposit taker, the resulting liquidity shortage could have serious adverse effects on activity in the wider economy.

During the Scoping phase, the entity and authorities may decide to also include non-critical – but from a business perspective important - functions within the scope of the test, in addition to the required critical functions.

The final TIBER-EU Scope Specification document should be agreed by the TCT during a workshop organised by the entity for all relevant stakeholders (i.e. WT, TCT and possibly the TI/RT providers). Importantly, the scope will need to be agreed at the board level of the entity. If the procurement has been completed, the scoping process and meeting may include the TI/RT providers.

The final TIBER-EU Scope Specification document to be provided by the entity will consist of the identified critical functions[3]; its sub-categories; their justification for inclusion; the identified key systems and services; and the “flags” to be captured.

[3] Complemented by identified non-critical, but important functions if agreed upon by the prospective tested entity and the respective TCT.

4 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. Only the key systems and services need to be included in the list below. **It is critical that the entity identifies key systems and services that are outsourced and cite to whom these are outsourced.**

The following is an example of systems and services used to deliver a critical function:

Critical Function ***(or sub-category)***	**System/service name**	**Present in jurisdiction**	**Justification for inclusion**
Deposit taking and savings ***(Retail internet banking)***	Customer Data Maintenance	XX	Within the deposit taking and savings services discharged by the bank, internet banking for retail customers is a core function, serving the real economy, and any disruption to this would have a detrimental impact on the customer base.
	Customer View	XX	
	Front-end Investments	YY	
	Front-end Payments	YY	
	TradeBox	XX	
	User Data Maintenance	YY	
	Logon	ZZ	

5 Setting the Flags

During the scoping process, the entity sets the “flags” to be captured, which are essentially the targets and objectives that the RT providers must strive to achieve during the test, using a variety of TTPs.

The WT should discuss the flags with the TCT, who must agree with them. Although the flags are set during the scoping process, they can be changed on an iterative basis following the threat intelligence gathering and as the red team test evolves.

During the process of setting the flags, the entity should analyse the systems and services used to discharge its critical functions, and thereafter consider what a real life attacker’s targets and objectives would be, to compromise the Confidentiality, Integrity and Availability (CIA) of the disclosed systems and services. This entails the entity to consider the primary risks to the business that could arise through the compromise of these systems or services (processes and/or people) and the foreseeable detrimental impact on the functioning of the entity and on financial stability.

It is critical that the entity identifies potential flags that may be set on outsourced functions, systems and services.

The following is an example of a flag and compromise action:

Flag XX:

Critical function *(sub-category)*	Deposit taking and savings *(Retail internet banking)*
Target System / Service name	Internet banking, consisting of: Customer Data Maintenance; Customer View; Front-end Payments; TradeBox; User Data Maintenance; and Logon
Information Assurance threat category (Confidentiality, Integrity, Availability)	Integrity
Description of system/service function	Core payment service
Objective - i.e. testing activity required to demonstrate compromise (e.g. Exfiltration, Insertion, Privilege Escalation)	Ability to initiate unauthorised credit transfer

6 Annex

The entity should complete the following tables, including the identified critical functions; its sub-categories; their justification for inclusion; the identified key systems and services; and the "flags" to be captured.

Whilst completing the table, the entity should not disclose its name but use the agreed upon code name for the TIBER-EU test.

Critical functions of [Code Name]:

Critical Function ***(or sub-category)***	**System/service name**	**Present in jurisdiction**	**Justification for inclusion**

Flag XX:

Critical function *(sub-category)*	
Target System / Service name	
Information Assurance threat category (Confidentiality, Integrity, Availability)	
Description of system/service function	
Objective - i.e. testing activity required to demonstrate compromise (e.g. Exfiltration, Insertion, Privilege Escalation)	

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