



**BANCA D'ITALIA**  
EUROSISTEMA

La resilienza cibernetica del sistema finanziario italiano: il ruolo dei test TIBER-IT

## **La metodologia TIBER-IT**

**finalità, modalità di svolgimento dei test e ruoli coinvolti presso gli operatori**

TIBER-IT Cyber Team

*Divisione Continuità di servizio del sistema finanziario  
Servizio Supervisione mercati e sistemi di pagamento*

*Milano – 13 ottobre 2022*

1

I test TLPT ed il TIBER-EU: contesto di riferimento

2

Il TIBER-IT: *timeline*, governance e processo

3

Il TIBER-IT: ruoli principali, responsabilità e prossimi passi

**1****I test TLPT ed il TIBER-EU: contesto di riferimento****2**

Il TIBER-IT: timeline, governance e processo

**3**

Il TIBER-IT: ruoli principali, responsabilità e prossimi passi

# I test TLPT ed il TIBER-EU: contesto di riferimento

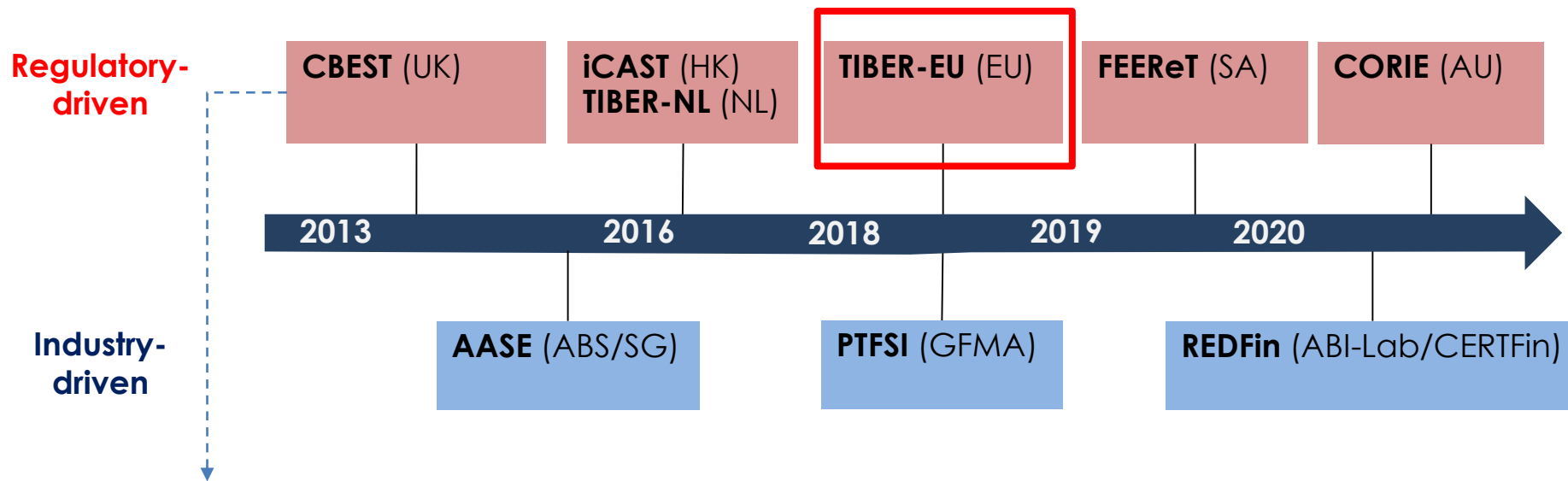
- ☐ Metodologie e strumenti per la conduzione di test avanzati di sicurezza: *Threat-led penetration testing (TLPT) o Red Teaming*



- ☐ “TLPT is a **controlled attempt** to compromise the cyber resilience of an entity by **simulating the tactics, techniques and procedures of real-life threat actors**. It is based on **targeted threat intelligence** and focuses on an entity’s people, processes and technology, with **minimal foreknowledge and impact on operations.**”

Fonti: [G7 Fundamental Elements for TLPT \(2018\)](#); [FSB Cyber Lexicon \(2018\)](#)

# I test TLPT ed il TIBER-EU: contesto di riferimento



- ❑ **Metodologia CREST/STAR** (*Simulated Targeted Attack and Response*)
- ❑ **Obbligatorio** per gli operatori di rilevanza sistemica
- ❑ **Benchmark iniziale** e riferimento metodologico per lo sviluppo di tutti gli altri framework
- ❑ **Processo su tre fasi** (*threat intelligence, testing, detection and response*) e **funzioni critiche** (CFs) da sottoporre a test concordate dall'inizio

Fonte: SCYTHE Platform - [Red Team and Threat-Led Penetration Testing Frameworks \(2020\)](#)

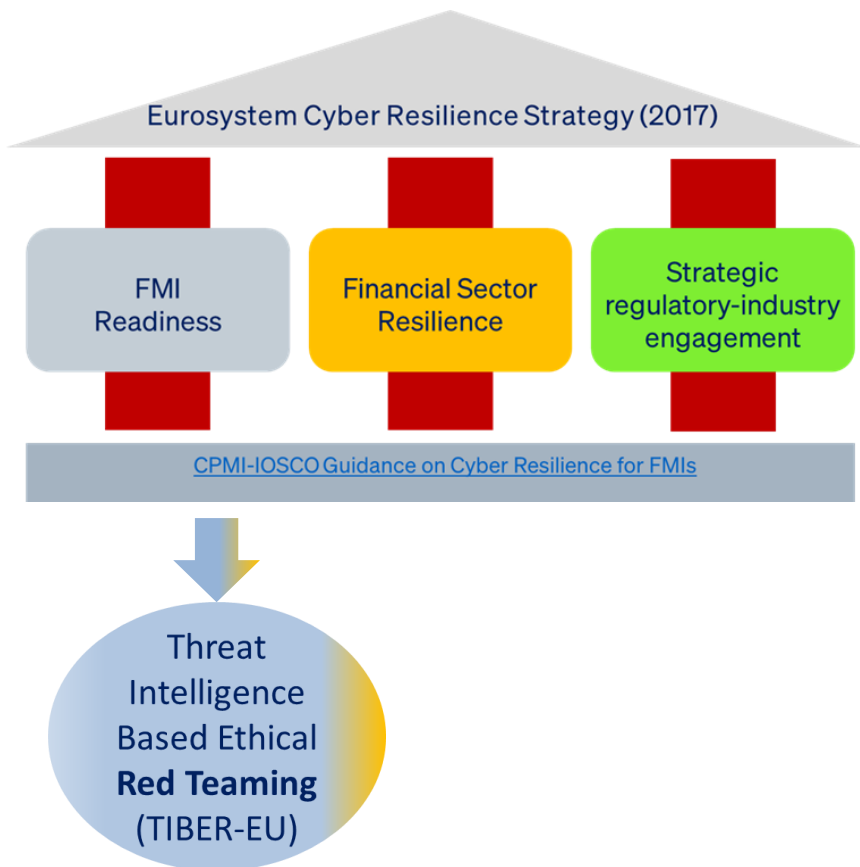
# I test TLPT ed il TIBER-EU: contesto di riferimento

#	Process Phase	Gap analysis of key requirements	CBEST	iCAST	TIBER-EU
1	Preparation	<b>Supervisory tool</b>	Red	Yellow	Green
2		Regulator approved	Red	Yellow	Red
3		Scoping based on Critical Functions	Red	Red	Red
4		Kill chain like process/end to end	Red	Red	Red
5		Scenario X	Yellow	Yellow	Green
6		Ongoing capability assessment ( Frequency)	Red	Yellow	Red
7	Testing (TI + RT)	Governmental TI check	Red	Yellow	Green
8		Target TI for sector/organization (TII)	Red	Red	Red
9		Generic TI for sector (GTL)	Green	Yellow	Green
10		Assessment of security testers (Certification, Experience)	Red	Red	Red
11		Accreditation scheme for security providers (e.g. CREST)	Red	Green	Red
12		Systematically Important Financial Entities	Red	Red	Green
13		<b>Live production systems</b>	Red	Red	Red
14		Physical & BYOD	Green	Green	Green
15		Third Party Service Provider testing	Red	Green	Red
16		Confidential testing (only White team)	Red	Red	Red
17		TCT from NCB/NCA	Red	Yellow	Red
18	Closure	Board engagement	Red	Green	Red
19		<b>Replay RT and BT to understand what happened</b>	Green	Yellow	Red
20		Purple teaming ( RED + BLUE Teaming)	Yellow	Yellow	Green
21		Details of Technical Vulnerabilities discovered	Yellow	Red	Red
22		Results and remediation's plans accessible to NCB/NCA	Red	Red	Red
23		Sharing lessons learned	Yellow	Yellow	Green
24		Thematic finding for the sector, shared by the Regulators	Red	Red	Green
25		Ev aluation framework & all party Feedback after the test	Red	Yellow	Red
26		KPI's	Yellow	Red	Yellow
27	<b>Attestation for the completed test</b>	Green	Yellow	Red	

Obbligatorio
Opzionale
Non Presente

- Ampia **convergenza** tra i framework
- Maggiore **allineamento** tra TIBER-EU e CBEST
- Maggior **numero di requisiti** in TIBER-EU (obbligatori e opzionali)
- Maggiore **flessibilità** in TIBER-EU e alcuni **requisiti obbligatori** in più rispetto al CBEST per recepimento nazionale e mutuo riconoscimento

# I test TLPT ed il TIBER-EU: contesto di riferimento



- ❑ Riferimento metodologico paneuropeo per la conduzione di test TLPT
- ❑ Sviluppato in **attuazione della Strategia di CR** dell'Eurosistema
- ❑ Inspirato da **CBEST e TIBER-NL (2016)** con **elementi di flessibilità** per il recepimento a livello nazionale
- ❑ Conduzione di **test cross-border** e il **mutuo riconoscimento dei risultati** attraverso al ricorso esclusivo a **tester esterni**
- ❑ Simulazione realistica per **identificare potenziali vulnerabilità** (*no pass or fail*)

## TIBER-EU

### Principali obiettivi

- ❑ **Incoraggiare** lo svolgimento di test TLPT
- ❑ **Armonizzare** e standardizzare
- ❑ **Svolgere** test cross-border
- ❑ **Facilitare** la collaborazione cross-authority
- ❑ **Assicurare** coerenza con i principi, le prassi internazionali

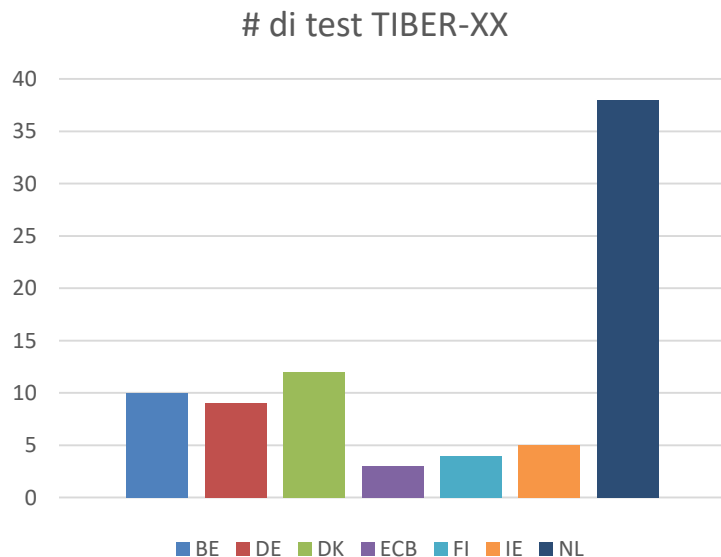
### Principi guida

- ❑ **Governance:** ruolo delle autorità
- ❑ **Assurance:** riconoscimento, accreditamento, attestazione
- ❑ **Compliance:** sicurezza, privacy, etica
- ❑ **Cooperation:** approccio di sistema
- ❑ **Sector resilience:** condivisione esperienze e lezioni apprese
- ❑ **Organisation-agnostic:** adattabile a qualsiasi organizzazione/settore



# I test TLPT ed il TIBER-EU: contesto di riferimento

- ❑ 13 giurisdizioni (+ECB) hanno adottato TIBER-EU
- ❑ 2 in fase di adozione (Austria e Francia)
- ❑ Al 2022, oltre 75 test TIBER



Fonte: [BCE/TKC](#), dati 2021



1

I test TLPT ed il TIBER-EU: contesto di riferimento

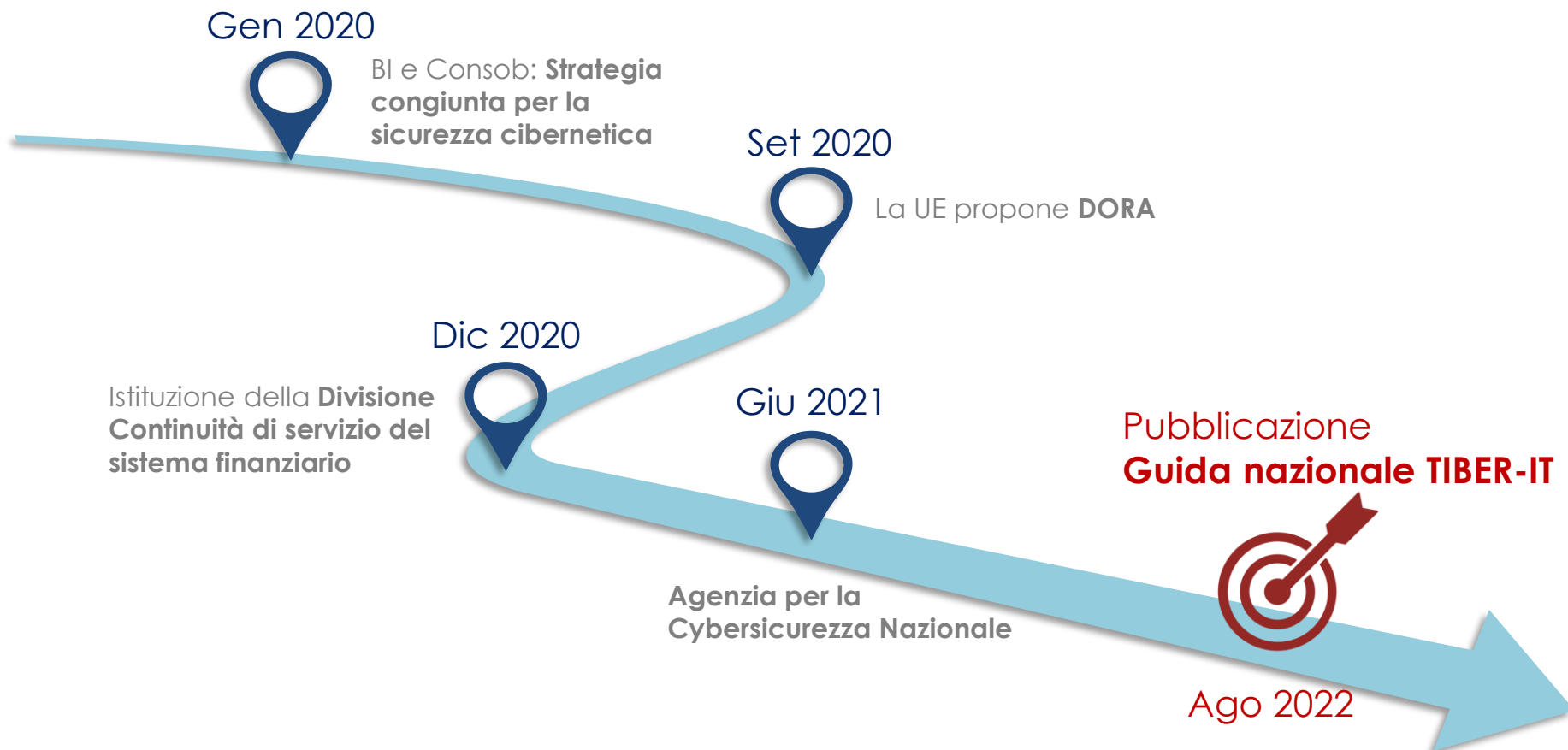
2

Il TIBER-IT: *timeline*, governance e processo

3

Il TIBER-IT: ruoli principali, responsabilità e prossimi passi

# Il TIBER-IT: *timeline*, governance e processo





- ❑ Approvata dai vertici delle 3 autorità e **pubblicata ad agosto 2022**
- ❑ **Passaggio formale e sostanziale** per il recepimento del framework TIBER-EU a livello nazionale
- ❑ **Riferimento metodologico** per la conduzione dei test TLPT da parte di:
  - ❑ infrastrutture del mercato finanziario
  - ❑ sistemi di pagamento e infrastrutture di supporto tecnologico o di rete
  - ❑ sedi di negoziazione
  - ❑ banche
  - ❑ istituti di pagamento e di moneta elettronica
  - ❑ intermediari finanziari ex art. 106 TUB
  - ❑ imprese di assicurazione
  - ❑ intermediari assicurativi

## Ruolo delle autorità finanziarie



Promuovere la **partecipazione** (su base **volontaria**) delle entità finanziarie ai test TIBER-IT

**Aggiornare il framework TIBER-IT** e condividere le lezioni apprese



**Definire la programmazione** annuale/pluriennale consultando le entità finanziarie che hanno espresso la loro disponibilità a sottoporsi ai test

**Fornire orientamenti e supporto** alle entità finanziarie in coordinamento con i principali stakeholder (es. la BCE e il **TIBER Knowledge Centre**)



## TIBER-IT Cyber Team (TCT)

- ❑ Team partecipato da **BI\***, **Consob** e **IVASS**
- ❑ **Aggiornamento e implementazione** del TIBER-IT
- ❑ **Pianificazione** di dettaglio dei test
- ❑ Mantiene i contatti con gli **altri TCT esteri e il TKC coordinato dalla BCE**
- ❑ SPOC per ogni **richiesta di informazione** sul TIBER-IT



[tiber-it@bancaditalia.it](mailto:tiber-it@bancaditalia.it)

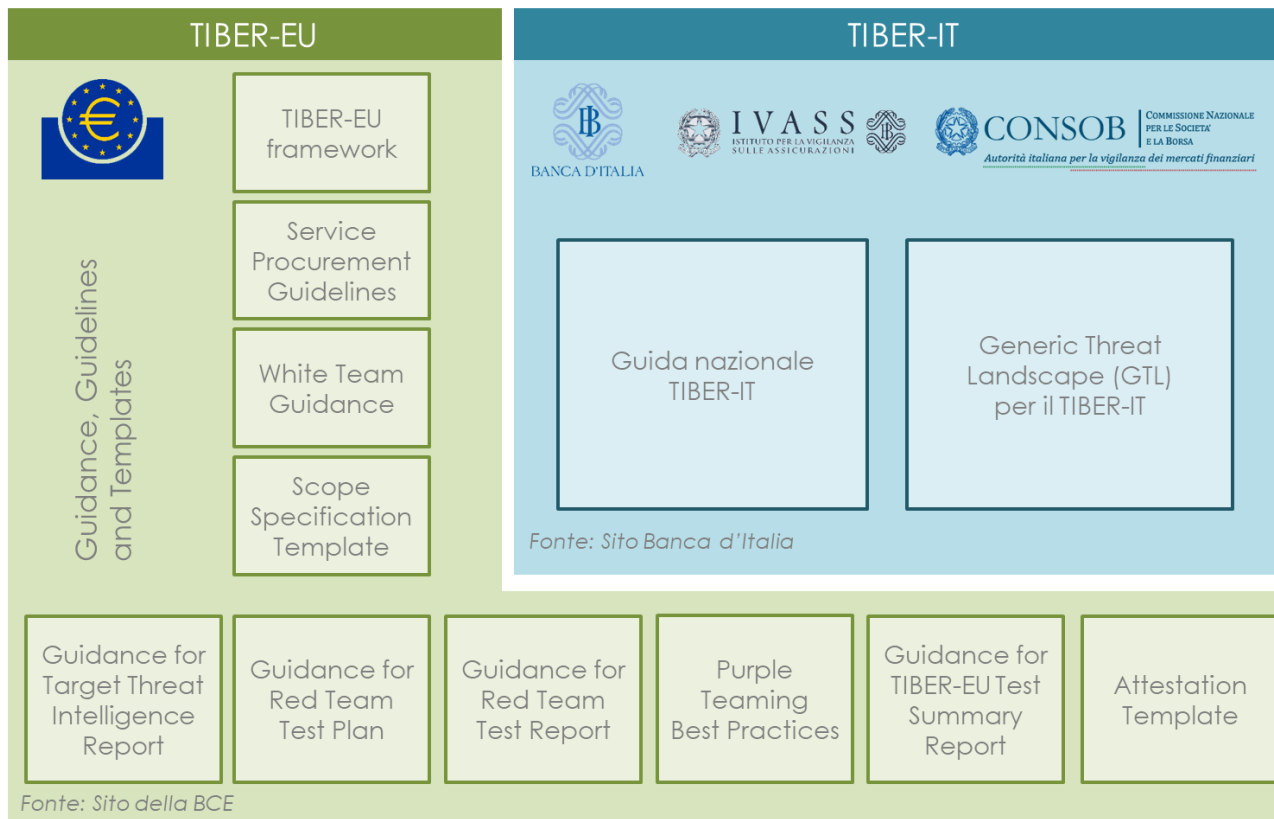
(\* ) DIVISIONE CONTINUITA' DI SERVIZIO DEL SISTEMA FINANZIARIO (SMP): supporto metodologico, amministrativo e operativo per il funzionamento del TIBER-IT e del TCT (esprime un nucleo stabile di risorse dedicate)

# Il TIBER-IT: *timeline*, governance e processo



→ **Generic Threat Intelligence (GTI)**: fase di produzione del **Generic Threat Landscape (GTL)**, elemento opzionale per i test ma ritenuto di valore.

# Il TIBER-IT: *timeline*, governance e processo





1

I test TLPT ed il TIBER-EU: contesto di riferimento

2

Il TIBER-IT: *timeline*, governance e processo

3

**Il TIBER-IT: ruoli principali, responsabilità e prossimi passi**

## ATTORI PRINCIPALI

Autorità competenti



Entità finanziaria soggetta a test



Fornitori di servizi esterni



## RUOLI

TIBER-IT Cyber Team (**TCT**)  
Team Test Manager (**TTM**)

White Team (**WT**)  
White Team Lead (**WTL**)  
Blue Team (**BT**)

Threat Intelligence (**TI**) Provider  
Red Team (**RT**) Provider

## AUTORITÀ

### TIBER-IT CYBER TEAM (TCT)

- ❑ **Esprime e supporta** il TTM
- ❑ Fornisce il **Generic Threat Landscape** *(se disponibile)*
- ❑ È informato sull'**evoluzione** del test

### TEAM TEST MANAGER (TTM)

- ❑ **Punto di contatto** con il WT/WTL
- ❑ Condivide lo **scope** del test
- ❑ Verifica che il test sia **aderente ai requisiti** TIBER-EU/IT
- ❑ Ha **contatti diretti** con TI/RT Providers



## ENTITÀ FINANZIARIA



### WHITE TEAM (WT)

- pianificazione** complessiva
- definizione dello **scope**
- gestione** di tutte le fasi del test
- acquisizione** dei servizi
- controllo dei **rischi**

### WHITE TEAM LEAD (WTL)

- Coordina** tutte le attività (day-by-day)
- Punto di contatto** con il TTM/TCT
- Interviene in caso di **escalation**

#### [TIBER-EU White Team Guidance](#)

- Unico** team che è **informato** del test, il più **ristretto** possibile
- Livello di **seniority** adeguato (include C-level)
- Competenze e profonda conoscenza dell'infrastruttura IT
- Eventualmente anche **esterni** (es. terze parti)

## FORNITORI ESTERNI



### THREAT INTELLIGENCE (TI) PROVIDER

- Raccoglie informazioni **mirate** (TTI)
- Adopera **varie fonti**
- Informazioni **up-to-date**



### RED TEAM (RT) PROVIDER

- Sviluppa gli **scenari** di attacco
- Prova a **violare** le difese
- Usa **TTPs** realistici



#### TIBER-EU Services Procurement Guidelines

- Referenze** a livello societario
- Esperienze** dei team incaricati
- Eventuali **certificazioni**
- Fiducia, etica** professionale
- Coperture **assicurative**

# Il TIBER-IT: ruoli principali, responsabilità e prossimi passi



## BLUE TEAM (BT)

- Tutto il resto del personale **non informato** del test
- Include lo staff responsabile per la **difesa dei sistemi informativi**
- Nella fase di chiusura del test **partecipa alla fase di replay**

## ENTITÀ FINANZIARIA



## PURPLE TEAM (PT)

[TIBER-EU Purple Teaming Best Practices](#)

# Il TIBER-IT: ruoli principali, responsabilità e prossimi passi

## PREPARATION



- Pre-launch
- Launch
- Scoping



- Test Project plan
- Scoping document
- GTL\**

\* *opzionale*

## TESTING

- TI scenario
- Handover
- Daily/Weekly updates

- TTI Report
- RT Test Plan
- RT Logs & Evidenze

## CLOSURE

- Replay Workshop
- 360° feedback
- PT Replay Workshop\**

- RT Report
- BT Report
- 360° feedback
- PT Report\**
- Test Summary Report
- Remediation Plan
- Attestazione TIBER-IT



## TIBER-IT

*Guida nazionale*

- ❑ Test su base **volontaria**
- ❑ Prioritariamente rivolto agli operatori più maturi e di **rilevanza sistemica**
- ❑ Utile in **preparazione** di DORA



## DORA

*Digital Operational Resilience Act*

- ❑ **Obbligatorietà** di Threat Led Penetration Testing (TLPT)
- ❑ Solo per **alcune** entità finanziarie identificate dalle NCA (secondo criteri da definire in RTS)
- ❑ **Esplicito riferimento a TIBER-EU** per lo sviluppo degli RTS



- ❑ **Pianificazione ed avvio dei primi test**
- ❑ **Ulteriori eventi** mirati di approfondimento e lezioni apprese dai test, anche in sedi cooperative pubblico-privato (es. Codise, CERTFin)
- ❑ Elaborazione del **GTL**
- ❑ **Consolidamento della collaborazione** tra le autorità responsabili del TIBER-IT

## Contatti



[Link alla pagina TIBER-IT](#)



[tiber-it@bancaditalia.it](mailto:tiber-it@bancaditalia.it)