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

Agenda

BANCA D'ITALIA
EUROSISTEMA

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

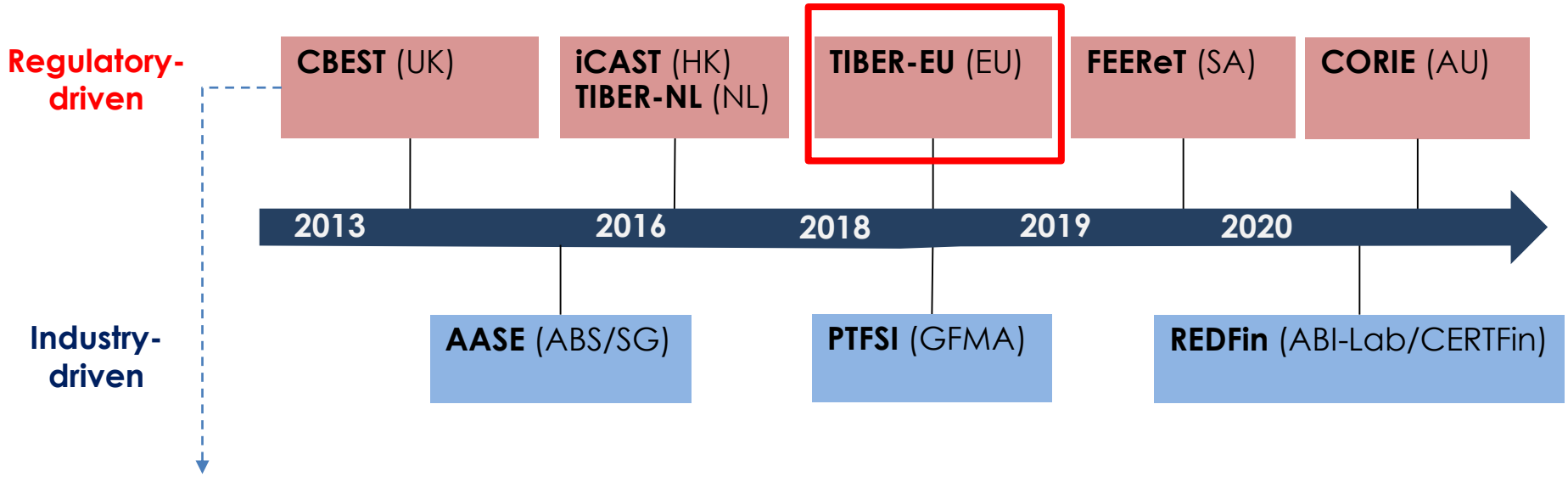
- Metodologie e strumenti per la conduzione di test avanzati di sicurezza: *Threat-led penetration testing* (TLPT) o *Red Teaming*

FSB FINANCIAL STABILITY BOARD

- "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

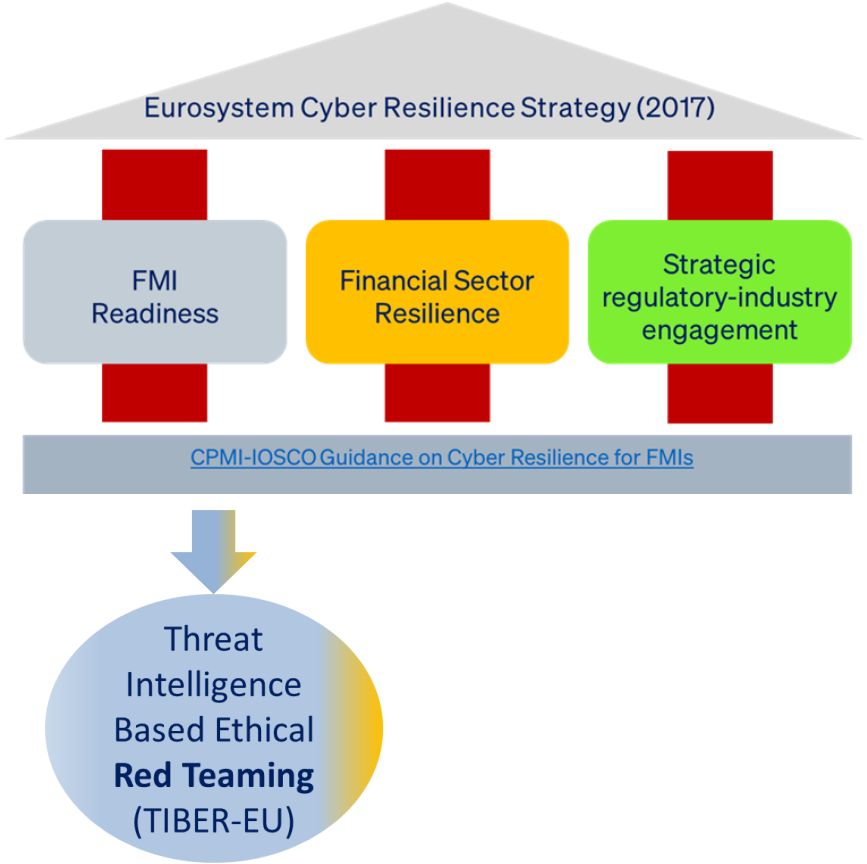
BANCA D'ITALIA
EUROSISTEMA

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

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*)

BANCA D'ITALIA
EUROSISTEMA

TIBER-EU

Principali obiettivi

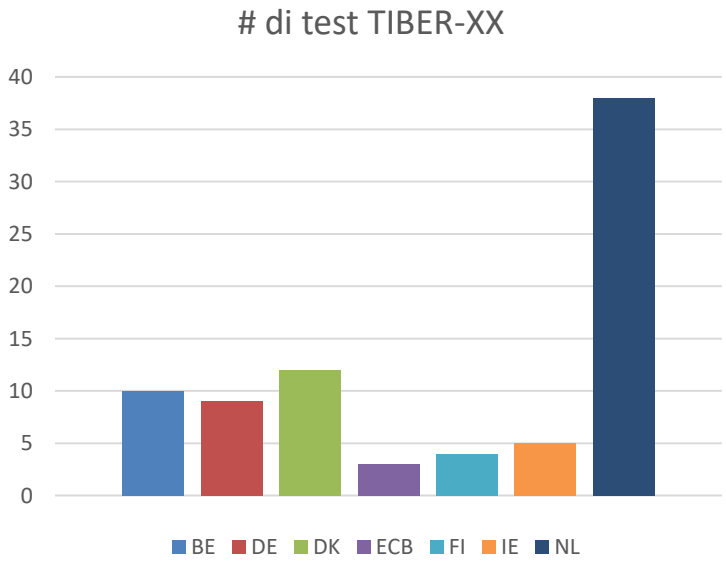
- **Incoraggiare** lo svolgimento di test TLPT
- **Armonizzare** e standardizzare
- **Svolgere** test cross-border
- **Facilitare** la collaborazione cross-authority
- **Assicurare** coerenza con i principi, le prassi internazionali

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**



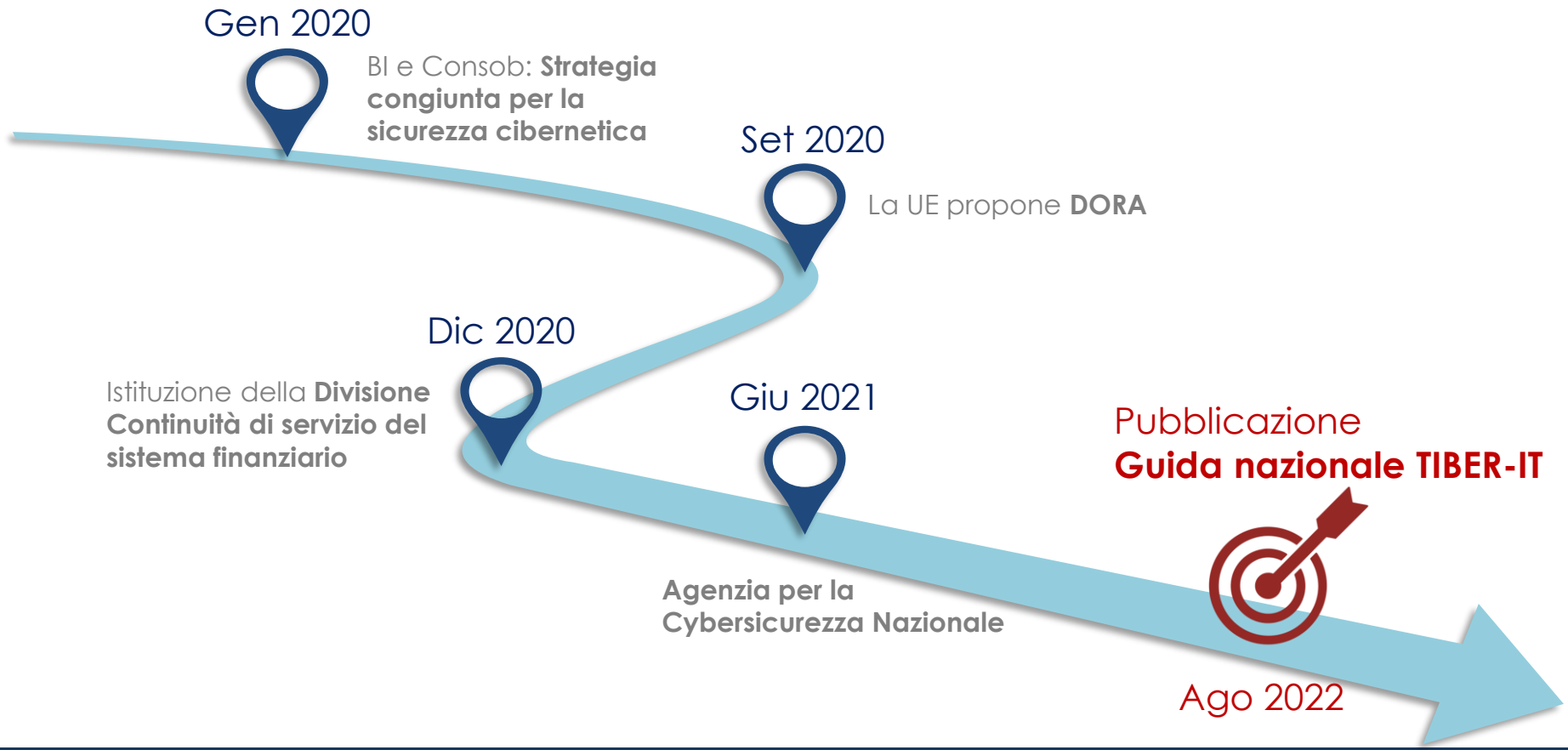
Fonte: BCE/TKC, dati 2021

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



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

BANCA D'ITALIA
EUROSISTEMA

CONSOB | COMMISSIONE NAZIONALE PER LE SOCIETÀ E LA BORSA
Autorità italiana per la vigilanza dei mercati finanziari

IVASS
ISTITUTO PER LA VIGILANZA SULLE ASSICURAZIONI

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

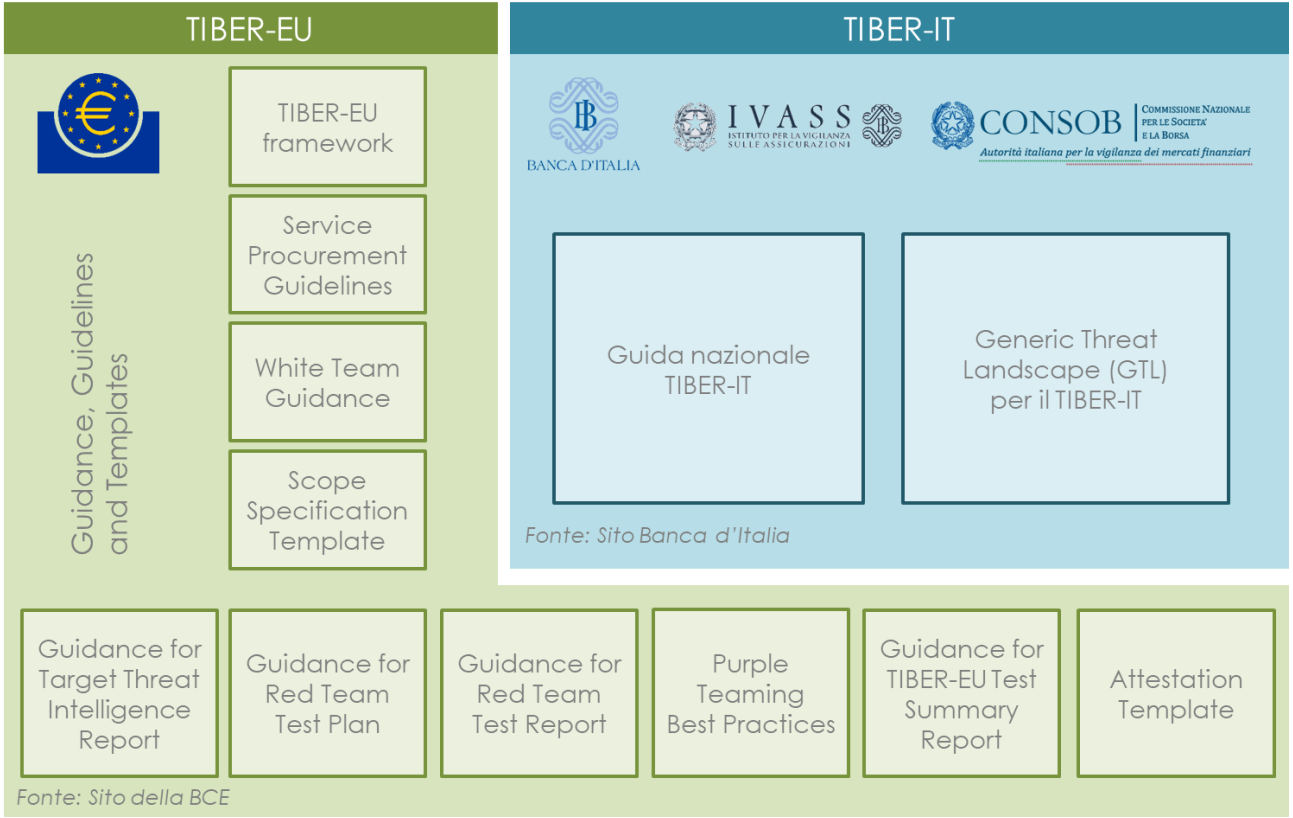
4-6 settimane
escluso procurement

15-17 settimane
(5 per TTI
10-12 per RT test)

4 settimane

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**

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

ATTORI PRINCIPALI		RUOLI
Autorità competenti		TIBER-IT Cyber Team (**TCT**) Team Test Manager (**TTM**)
Entità finanziaria soggetta a test		White Team (**WT**) White Team Lead (**WTL**) Blue Team (**BT**)
Fornitori di servizi esterni		Threat Intelligence (**TI**) Provider Red Team (**RT**) Provider

BANCA D'ITALIA
EUROSISTEMA

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)

BANCA D'ITALIA
EUROSISTEMA

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

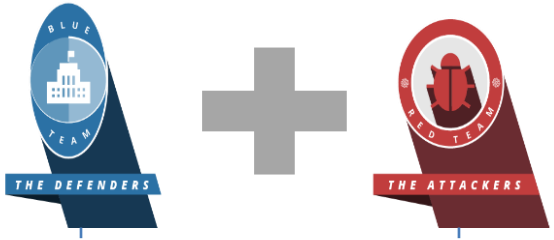
TIBER-EU Services Procurement Guidelines

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

ENTITÀ FINANZIARIA

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**



PURPLE TEAM (PT)

TIBER-EU Purple Teaming Best Practices

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

BANCA D'ITALIA
EUROSISTEMA

PREPARATION

- ❑ Pre-launch
- ❑ Launch
- ❑ Scoping

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

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

** opzionale*

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

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

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

- **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

BANCA D'ITALIA
EUROSISTEMA

Contatti

Link alla pagina TIBER-IT

tiber-it@bancaditalia.it