CONSOB
Commissione Nazionale per le Società e la Borsa

BANCA D'ITALIA
EUROSISTEMA

IVASS
Istituto per la Vigilanza sulle Assicurazioni

Guida nazionale TIBER-IT

Threat Intelligence Based Ethical Red-Teaming – Italia

Novembre 2025 - versione 2.0

Grafica e stampa a cura della Divisione Editoria e stampa della Banca d'Italia

Francesco Trombadori, *Mattino a Ponte Fabricio*, Collezione Banca d'Italia

INDICE

1 Introduzione

1.1 Prefazione e inquadramento normativo

La resilienza operativa digitale delle singole istituzioni finanziarie e del sistema finanziario nel suo complesso rappresenta una priorità per gli operatori e per le Autorità a livello nazionale, europeo e internazionale. Ciò è dovuto alla crescente digitalizzazione e interconnessione del sistema finanziario, all'evoluzione dei mercati e dei modelli di business, dei canali di offerta e delle abitudini di utenti e clienti nella fruzioni dei servizi finanziari, alla centralità dei fornitori e alla complessità della relativa catena di fornitura. Inoltre, rilevano sia il mutato contesto geo-politico sia l'aumento e la sofisticazione degli attacchi cyber.

In tale quadro, il rafforzamento della resilienza operativa digitale beneficia del miglioramento della capacità di rilevamento, protezione e risposta agli attacchi cyber, sia a livello di singole entità sia a livello di sistema finanziario nel suo complesso. Tale risultato può essere raggiunto con l'utilizzo di test avanzati di cybersicurezza guidati dalla minaccia, i cc.dd. *Threat-Led Penetration Testing* (TLPT), introdotti nel sistema finanziario europeo nel 2018, attraverso il *framework* armonizzato TIBER-EU[1] per lo svolgimento di test su base volontaria.

A livello nazionale, la Banca d'Italia, la Commissione Nazionale per le società e la Borsa (Consob) e l'Istituto per la Vigilanza sulle Assicurazioni (Ivass) collaborano per migliorare la resilienza complessiva del sistema finanziario italiano e in tale quadro hanno adottato congiuntamente nel 2022 la Guida Nazionale TIBER-IT per lo svolgimento dei test di tipo volontario, in recepimento del *framework* TIBER-EU[2]. Tale guida era indirizzata prioritariamente agli operatori a rilevanza sistemica del sistema finanziario italiano con lo scopo di innalzare la stabilità complessiva, l'efficienza e la competitività del sistema finanziario[3], oltre che il regolare funzionamento, l'affidabilità e l'efficienza del sistema dei pagamenti[4].

Dal gennaio 2025 è applicabile il Regolamento (UE) 2022/2554 (*Digital Operational Resilience Act* – DORA)[5], che prevede come obbligatorio l'uso dei TLPT[6] come strumento di supervisione per verificare la resilienza operativa digitale delle entità finanziarie di maggiore rilevanza per il sistema finanziario.

---

1 Nel 2018 la BCE ha pubblicato la prima versione del *framework* TIBER-EU, strumento che simula potenziali attacchi cyber riproducendo tattiche, tecniche e procedure (TTP) di attori della minaccia reali (https://www.ecb.europa.eu/paym/cyber-resilience/tiber-eu/html/index.en.html).

2 https://www.bancaditalia.it/compiti/sispaga-mercati/tiber-it/index.html.

3 Cfr. art. 5, comma 1, d.lgs. 385/1993 (Testo Unico Bancario – TUB), art. 5, comma 1, d.lgs. 58/1998 (Testo Unico della Finanza – TUF) e art. 3, comma 1, d.lgs. 209/2005 (Codice delle Assicurazioni Private- CAP).

4 Cfr. art. 146, comma 1, TUB.

5 Il testo vigente è disponibile sul sito internet EurLex (https://eur-lex.europa.eu/eli/reg/2022/2554/oj). Gli eventuali aggiornamenti, conseguenti a successive modifiche e correzioni, saranno parimenti visibili sul sito EurLex, nella sezione "testi consolidati" (https://eur-lex.europa.eu/collection/eu-law/consleg.html?locale=it).

6 Cfr. artt. 26, che disciplina i "*Test avanzati di strumenti, sistemi e processi di TIC basati su test di penetrazione guidati dalla minaccia (TLPT)*", e 27, che stabilisce i "*Requisiti per i soggetti incaricati dello svolgimento dei test per lo svolgimento dei TLPT*".

Le entità finanziarie per le quali i TLPT sono obbligatori sono identificate dalle Autorità competenti secondo criteri quali-quantitativi definiti nel Regolamento Delegato (UE) 2025/1190, basato sulle norme tecniche di regolamentazione (cc. dd. *Regulatory Technical Standards* - RTS sui TLPT)[7], elaborate conformemente al TIBER-EU. A tal proposito, il *framework* TIBER-EU è stato recentemente aggiornato[8] per adeguarlo alle novità introdotte da DORA.

A livello nazionale, l'adeguamento a DORA è stato realizzato con il d.lgs. 23/2025[9], che designa come Autorità competenti *"per il rispetto degli obblighi posti dal medesimo regolamento a carico dei soggetti vigilati dalle medesime autorità, secondo le rispettive attribuzioni di vigilanza"*, la Banca d'Italia, la Consob e l'Ivass[10]. Dette attribuzioni riguardano anche lo svolgimento dei TLPT[11]. Per le banche significative l'Autorità competente è la BCE.

In relazione a quanto sopra, la Guida Nazionale TIBER-IT ("Guida") è stata integrata e aggiornata per tener conto delle previsioni di DORA, dell'RTS sui TLPT e delle novità introdotte dalla nuova versione del *framework* TIBER-EU, nonché dalle richiamate disposizioni nazionali.

La Guida offre una metodologia e un modello operativo utilizzabili sia per i test di tipo volontario sia per i TLPT obbligatori ai sensi di DORA, questi ultimi svolti dalle entità finanziarie identificate da Banca d'Italia, Consob e Ivass, secondo le rispettive attribuzioni.

1.2 Definizioni

Nel resto del documento, se non diversamente specificato, con il termine:

- "le Autorità" si intendono la Banca d'Italia, la Consob e l'Ivass;
- "Autorità competente" si intende l'autorità ex art. 46 del reg. DORA;
- "Autorità TIBER" si intende l'autorità competente che svolge le attività collegate a un test TIBER-IT o l'autorità a ciò delegata ai sensi dell'art. 26 par. 10 del reg. DORA sulla base degli accordi a livello nazionale tra le Autorità. Nel caso il test TIBER-IT sia svolto ai sensi di DORA, l'Autorità TIBER è considerata anche quale relativa "Autorità TLPT", come definita nell'RTS sui TLPT (cfr. §2.1.2);

---

7 Regolamento delegato (UE) 2025/1190. Il testo vigente è disponibile sul sito internet EurLex (https://eur-lex.europa.eu/eli/reg_del/2025/1190/oj). Gli eventuali aggiornamenti, conseguenti a successive modifiche e correzioni, saranno parimenti visibili sul sito EurLex, nella sezione "testi consolidati" (https://eur-lex.europa.eu/collection/eu-law/consleg.html?locale=it). Nella presente Guida, con RTS sui TLPT si fa riferimento al testo del citato Regolamento delegato.

8 https://www.ecb.europa.eu/press/intro/news/html/ecb.mipnews250211.en.html.

9 Decreto legislativo 10 marzo 2025, n. 23. Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2022/2554, relativo alla resilienza operativa digitale per il settore finanziario e che modifica i regolamenti (CE) n. 1060/2009, (UE) n. 648/2012, (UE) n. 600/2014, (UE) n. 909/2014 e (UE) 2016/1011, e per il recepimento della direttiva (UE) 2022/2556, che modifica le direttive 2009/65/CE, 2009/138/CE, 2011/61/UE, 2013/36/UE, 2014/59/UE, 2014/65/UE, (UE) 2015/2366 e (UE) 2016/2341 per quanto riguarda la resilienza operativa digitale per il settore finanziario.

10 Cfr. art. 3.

11 L'Italia non ha esercitato l'opzione prevista dall'art. 26 par. 9 di DORA di designare un'autorità pubblica unica nel settore finanziario responsabile delle questioni relative ai TLPT nel settore finanziario a livello nazionale.

- "entità finanziarie" si comprendono:
  i. le entità finanziarie come definite nell'art. 2, par. 2 del reg. DORA di competenza delle Autorità;
  ii. i sistemi di pagamento;
  iii. le infrastrutture di supporto tecnologico o di rete[12];
  iv. Poste Italiane S.p.A., per le attività di Bancoposta di cui al decreto del Presidente della Repubblica 14 marzo 2001, n. 144[13];
  v. gli intermediari finanziari ex art. 106 TUB;
- "settore finanziario" si comprendono le entità finanziarie sopra descritte.

1.3 Ambito di applicazione

La Guida è indirizzata alle entità finanziarie, sia per i TLPT obbligatori ai sensi di DORA sia per i test su base volontaria, ai loro fornitori di servizi ICT (laddove inclusi nel perimetro del test), ai fornitori di servizi di analisi della minaccia (*threat intelligence* - TI) e ai *red team testers* (RTT).

Tuttavia, anche altre entità finanziarie e/o altre tipologie di soggetti[14] possono comunicare al punto di contatto unico per ogni richiesta relativa al TIBER-IT, rappresentato dal seguente indirizzo e-mail: tiber-it@bancaditalia.it, l'interesse a svolgere un test volontario. In tal caso, se ne valuterà l'opportunità nell'ottica di un complessivo innalzamento della resilienza del settore finanziario tenendo conto, ad esempio, delle loro interconnessioni con altre entità finanziarie, della loro maturità cyber, oltre che della propria disponibilità di risorse per la supervisione del test stesso.

Con riguardo alle banche significative la Guida non si applica ai TLPT obbligatori ai sensi di DORA, per i quali si deve far riferimento a quanto stabilito nell'ambito del Meccanismo di vigilanza unico (*Single Supervisory Mechanism* - SSM), mentre resta valida per i test a carattere volontario.

1.4 Cos'è il TIBER-IT

Il TIBER-IT recepisce a livello nazionale il *framework* TIBER-EU, tenendo conto delle specificità nazionali; le indicazioni in esso contenute sono volte ad assicurare il riconoscimento dei test da parte delle altre giurisdizioni che recepiscono il TIBER-EU, nonché a fornire indicazioni pratiche per lo svolgimento di TLPT ai sensi di DORA.

---

12 Per "infrastrutture di supporto tecnologico o di rete" si intende il complesso di impianti e di implementazioni a supporto di uno o più servizi strumentali al sistema dei pagamenti, tra i quali a titolo di esempio: a) servizi di messaggistica e di rete; b) servizi e/o applicazioni di business strumentali a trattamento e scambio di flussi finanziari e informativi, compensazione e/o regolamento di operazioni di pagamento (vedasi per dettagli le "Disposizioni in materia di sorveglianza sui sistemi di pagamento e sulle infrastrutture strumentali tecnologiche o di rete" emanate da Banca d'Italia il 9 novembre 2021).

13 L'applicazione a Bancoposta di alcuni articoli di DORA è stata prevista dal d.lgs. 23/2025.

14 Ad esempio, soggetti coinvolti in attività rilevanti per il sistema finanziario.

Tramite l'esecuzione di test TIBER-IT le entità finanziarie possono migliorare la propria resilienza operativa e le Autorità possono ottenere, anche ai fini della stabilità finanziaria, un'adeguata assicurazione relativa alla postura di resilienza cyber sia a livello di singola entità sia a livello settoriale.

Durante tutto il processo, i test TIBER-IT prevedono un forte coinvolgimento di tutti i portatori di interesse (approccio *multi-stakeholder*). Le entità sottoposte al test individuano le principali parti interessate da coinvolgere nel test. Poiché i TLPT sono strumenti intrusivi e da condurre in ambiente di produzione, tutte le parti interessate, il *management* aziendale e in particolare il *Control Team* (CT, cfr. §2.2.1) devono attribuire la massima priorità alla chiara definizione del perimetro di applicazione (*scope*) del test, individuando le funzioni critiche[15] (FC) da includere nel test, e all'applicazione di controlli efficaci per la gestione dei rischi per tutta la durata del processo.

In questo contesto la Banca d'Italia riveste il ruolo di Autorità capofila del TIBER-IT e svolge le attività di sua competenza in stretta collaborazione con la Consob e l'Ivass.

La revisione del TIBER-IT e il suo allineamento con il TIBER-EU, il regolamento DORA e le altre migliori pratiche internazionali sono guidati da un gruppo di coordinamento interistituzionale tra le tre Autorità (TLPT *Steering Committee*, cfr. §2.1.1).

1.5 I TLPT obbligatori ai sensi di DORA e i test volontari

Il regolamento DORA (artt. 26 e 27) prevede l'obbligo di effettuare test di penetrazione guidati dalla minaccia (TLPT) per le entità finanziarie identificate come critiche o aventi un potenziale impatto sistemico. Come detto, in Italia tali entità sono individuate dalle rispettive Autorità competenti, ovvero la Banca d'Italia, la Consob e l'Ivass, sulla base delle rispettive attribuzioni previste dall'ordinamento; mentre per le banche classificate come significative l'Autorità competente è la BCE.

La metodologia di svolgimento di un TLPT ai sensi di DORA, illustrata in dettaglio nell'RTS sui TLPT, è stata sviluppata in conformità al *framework* TIBER-EU. Il TIBER-EU, così come l'implementazione nazionale TIBER-IT di cui alla presente Guida possono, quindi, essere considerati conformi ai requisiti sui TLPT di DORA. Sia il TIBER-EU che il TIBER-IT sono guide operative che forniscono indicazioni metodologiche[16].

---

15 Nel prosieguo del documento i termini funzione critica o funzione essenziale o importante (FEI) sono intercambiabili. Il Regolamento DORA (art. 3, n. 22) definisce una FEI come "una funzione la cui interruzione comprometterebbe sostanzialmente i risultati finanziari di un'entità finanziaria o ancora la solidità o la continuità dei suoi servizi e delle sue attività, o la cui esecuzione interrotta, carente o insufficiente comprometterebbe sostanzialmente il costante adempimento, da parte dell'entità finanziaria, delle condizioni e degli obblighi inerenti alla sua autorizzazione o di altri obblighi previsti dalla normativa applicabile in materia di servizi finanziari".

16 Si veda anche la pubblicazione della BCE di settembre 2024: "*Adopting TIBER-EU will help fulfil DORA requirements*", https://www.ecb.europa.eu/press/intro/publications/pdf/ecb.miptopical240926.en.pdf.

Il regolamento DORA e il relativo RTS sui TLPT stabiliscono il quadro regolamentare di riferimento e delineano i requisiti normativi del TLPT, mentre il TIBER-EU e il TIBER-IT forniscono un supporto metodologico su come un TLPT debba essere condotto sia dall'entità testata sia dalle Autorità.

In considerazione dell'allineamento tra il TIBER-EU e i TLPT ai sensi di DORA, il TIBER-IT rappresenta il modello di riferimento per l'effettuazione di TLPT obbligatori ai sensi di DORA per le entità finanziarie individuate dalle Autorità competenti.

Nel caso di TLPT svolto ai sensi di DORA, l'Autorità competente identifica l'entità finanziaria obbligata a svolgere i test mediante formale comunicazione[17]. Successivamente, l'Autorità TIBER notificherà all'entità finanziaria l'inizio del test (cfr. §4.1).

Le entità finanziarie non obbligate a svolgere un TLPT possono manifestare l'interesse a partecipare volontariamente a un test TIBER-IT comunicandolo al punto di contatto unico (cfr. §1.3). In tal caso, la decisione di partecipare al test dovrebbe essere presa a livello di Consiglio di Amministrazione o di organo analogo dell'entità finanziaria o di un soggetto a ciò appositamente delegato.

Le differenze tra un TLPT ai sensi di DORA e un test volontario risiedono, sostanzialmente, nell'obbligatorietà e nell'utilizzo del primo anche come strumento di vigilanza prudenziale. Il processo di esecuzione del singolo test è il medesimo e lo scopo principale è quello di innalzare la resilienza cyber dell'entità testata, anche facendo leva sulle occasioni di apprendimento sperimentate nel corso del test.

A tal fine, oltre a quanto stabilito nei successivi capitoli di questa Guida, nel framework TIBER-EU e nei relativi documenti accessori[18], è necessario rispettare le previsioni contenute in DORA e nel relativo RTS sui TLPT, nella versione vigente al momento dello svolgimento del test.

In conformità al *framework* TIBER-EU e alle disposizioni contenute in DORA, infine, è prevista la possibilità di effetture TLPT di tipo transfrontaliero e/o TLPT che coinvolgono più entità finanziarie, specie nel caso di entità con operatività in più Paesi e/o che condividono la medesima infrastruttura tecnologica o gli stessi fornitori ICT: il cc.dd. *multiparty testing*[19], che include i *joint test* e i *pooled test*[20].

1.6 Nota legale

Le informazioni e le indicazioni espresse in questa Guida sono fornite a scopo informativo e non intendono costituire un'interpretazione legale o di altro tipo.

---

17 I dettagli del processo di identificazione non sono inclusi nella presente Guida.

18 Cfr. §9.2. La documentazione supplementare è aggiornata e pubblicata dalla BCE sul proprio sito istituzionale.

19 Cfr. anche il par. 3.10 del TIBER-EU.

20 Cfr. rispettivamente l'art. 1.18 dell'RTS sui TLPT (*joint TLPT*) e l'art. 26.4 di DORA.

Si raccomanda di consultare il *framework* TIBER-EU oltre alla presente Guida, in quanto sono complementari: la Guida TIBER-IT non fornisce una descrizione approfondita di tutte le nozioni e di tutti i processi tratti dal *framework* TIBER-EU, dove sono invece già stati presentati in modo esauriente.

Per quanto non espressamente previsto dalla presente Guida si rinvia a quanto stabilito in DORA, nell'RTS sui TLPT, nel *framework* TIBER-EU e negli annessi documenti accessori. I relativi riferimenti e rinvii contenuti nella presente Guida si intendono effettuati alla versione vigente tempo per tempo. Eventuali successivi aggiornamenti del *framework* TIBER-EU e dell'RTS sui TLPT saranno automaticamente applicabili in virtù dei relativi rinvii contenuti nella presente Guida.

Ogni partecipante a un test TIBER-IT è l'unico ed esclusivo responsabile per l'esecuzione delle attività assegnategli dalla presente Guida, compresa la conformità alle leggi e ai regolamenti applicabili.

Le entità testate restano in ogni momento pienamente responsabili dei rischi associati alla conduzione del test e di qualsiasi impatto negativo sui loro servizi e verso i soggetti terzi.

La presente Guida nazionale recepisce il framework TIBER-EU.

2 Attori principali, ruoli, responsabilità e interazioni del TIBER-IT

Di seguito sono descritti i principali attori, ruoli, responsabilità e le interazioni tra le parti interessate (*stakeholders)* coinvolte nelle attività di gestione e implementazione del TIBER-IT e nel singolo test[21].

In relazione al singolo test, i principali portatori di interesse sono informati sui rispettivi ruoli e responsabilità. Occorrerà garantire che:

- il test sia condotto in modo controllato adottando un approccio basato sul rischio;
- venga stabilito un protocollo tra le parti interessate che definisca i flussi di informazione durante tutto lo svolgimento del test, nonché
- le modalità di archiviazione e condivisione delle informazioni.

2.1 Le Autorità

Le Autorità svolgono un ruolo sia nell'implementazione e nella revisione del TIBER-IT sia nella supervisione del processo di esecuzione del singolo test:

- attraverso la partecipazione al Gruppo di coordinamento sul TLPT per il sistema finanziario italiano (TLPT *Steering Committee for the Italian financial sector*, TLPT SC);
- in qualità di Autorità TIBER;
- costituendo il TIBER *Cyber Team*[22] (TCT) e designando il *Test Manager* (TM).

2.1.1 Gruppo di coordinamento sul TLPT per il sistema finanziario italiano (TLPT *Steering Committee for the Italian financial sector*, TLPT SC)

Per assicurare il coordinamento tra le Autorità, l'aggiornamento e l'implementazione del TIBER-IT opera un comitato di alto livello tra Banca d'Italia, Consob e Ivass, denominato Gruppo di coordinamento sul TLPT per il sistema finanziario italiano (TLPT SC), evoluzione del precedente Gruppo di coordinamento per il TIBER-IT istituito con l'adozione nel 2022 della Guida nazionale TIBER-IT.

2.1.2 Autorità TIBER (TIBER *Authority*)

L'Autorità TIBER:

- è una delle Autorità che ha adottato il TIBER-IT e che svolge attività specifiche nell'ambito di un test TIBER;

---

21 Nel prosieguo del documento, si fa riferimento indistintamente a "test", "test TIBER-IT", "TLPT", considerando che il processo di test è sostanzialmente il medesimo.

22 Nella presente Guida si può far riferimento indistintamente al TIBER Cyber Team o al TLPT Cyber Team.

- nel caso il test sia svolto ai sensi di DORA, è considerata anche come la relativa "Autorità TLPT[23]";
- nell'eventualità dell'esercizio della delega prevista ai sensi dell'art. 26 par. 10 del reg. DORA, coincide con l'autorità delegata.

Nel caso di *multiparty testing* è possibile che siano presenti più Autorità TIBER, anche di altri Paesi.

Le Autorità TIBER promuovono lo svolgimento da parte delle entità finanziarie di test TIBER-IT, ne indirizzano la relativa programmazione annuale e pluriennale e forniscono orientamenti e supporto metodologico per lo svolgimento del test.

Per lo svolgimento coordinato dei compiti assegnati alle Autorità TIBER è istituito un *TIBER-IT Cyber Team* (cfr. §2.1.3).

2.1.3 TIBER-IT *Cyber Team* (TCT) e *Test Manager* (TM)

Il TIBER-IT *Cyber Team* (TCT) è composto da rappresentanti delle Autorità che adottano la presente Guida ed è supportato da un gruppo stabile di risorse assicurate dalla Banca d'Italia.

Il TCT mantiene i contatti con i TCTs di altre autorità e/o Paesi e con il *Tiber Knowledge Centre* (TKC)[24] su base continuativa. Per ulteriori dettagli sul ruolo del TCT si rimanda al par. 3.2 del *framework* TIBER-EU.

Per ogni test è designato un *Test Manager* (TM), di norma tra il personale che compone il TCT, coadivuato da uno o più sostituti. Compito principale del TM è di seguire lo svolgimento del test da parte dell'entità testata e verificare nel continuo che la stessa effettui il test in modo controllato e in conformità con la presente Guida e il *framework* TIBER-EU. Il TM non è responsabile delle azioni del Control Team, dello svolgimento del test, dei risultati o del piano di rimedio (*Remediation Plan*).

Per ulteriori dettagli sul ruolo del TM si rimanda al par. 3.3 del *framework* TIBER-EU e alle sezioni relative a tutte le fasi del processo.

2.2 Le entità testate e i fornitori

Nell'ambito di un test i principali attori coinvolti sono:

- il *Control Team* (CT) e il *Control Team Lead* (CTL) dell'entità testata;
- il *Blue Team* (BT) dell'entità testata;

---

23 L'art. 1, n. (7) dell'RTS sui TLPT definisce "autorità competente per il TLPT" come: "*(a) […]; (b) l'autorità nel settore finanziario alla quale è delegato l'esercizio di alcuni o di tutti i compiti relativi ai TLPT conformemente all'articolo 26, paragrafo 10, del regolamento (UE) 2022/2554; (c) una qualsiasi delle autorità competenti di cui all'articolo 46 del regolamento (UE) 2022/2554*".

24 Istituito presso la BCE, il TKC è un forum composto da rappresentanti delle istituzioni che hanno recepito il framework TIBER-EU. I suoi obiettivi principali sono: i) manutenere il framework TIBER-EU; ii) facilitare il trasferimento di conoscenze e promuovere la collaborazione tra le varie giurisdizioni; iii) supportare le istituzioni nelle loro implementazioni nazionali e fornire un archivio centralizzato per i relativi documenti; iv) monitorare le implementazioni nazionali al fine di assicurare il mutuo riconoscimento dei test TIBER.

- il fornitore di servizi di analisi della minaccia (*Threat Intelligence Provider* – TIP);
- il *Red Team Tester* (RTT), che può essere un fornitore di servizi esterni o personale interno all'entità testata.

2.2.1 *Control Team* (CT) e *Control Team Lead* (CTL)

Per ogni test, l'entità testata stabilisce un *Control Team* (CT), guidato da un apposito *Control Team Lead* (CTL). Il CTL è una figura chiave per il corretto svolgimento del test e perciò è di norma nominato anche un suo sostituto. Il CTL è responsabile, tra l'altro, della definizione del perimetro di test e dell'esecuzione del test nel suo complesso.

Per ulteriori dettagli sul ruolo del CT e del CTL si rimanda al par. 3.4 del *framework* TIBER-EU e nelle sezioni relative a tutte le fasi del processo. Maggiori informazioni sui ruoli, le responsabilità e la composizione del CT sono presenti anche nel documento TIBER-EU *Control Team Guidance*.

2.2.2 *Blue Team* (BT)

Per ogni test, il *Blue Team* (BT) è composto da tutto il personale (non membro del CT) dell'entità testata, comprese le terze parti, specialmente coloro che gestiscono i sistemi (e le relative persone, processi e tecnologie) dell'entità testata.

In particolare, il BT include anche il personale responsabile della difesa della rete e dei sistemi informativi dell'entità. È fondamentale che il BT non sia a conoscenza del test durante il suo svolgimento e sia completamente estraneo alla preparazione e all'esecuzione del test.

Per ulteriori dettagli sul ruolo del BT si rimanda al par. 3.5 del *framework* TIBER-EU.

2.2.3 Fornitore di *threat intelligence* (TIP)

Il *Threat Intelligence Provider* (TIP) è un fornitore esterno i cui servizi di analisi della minaccia sono stati acquisiti dal CT in linea con gli standard e i requisiti minimi stabiliti nel documento TIBER-EU *Guidance for Service Provider Procurement*. Il TIP raccoglie informazioni mirate sull'entità testata, emulando la ricerca che sarebbe eseguita da un attaccante esperto e sviluppa degli scenari della minaccia specifici per l'entità testata. Il TIP dovrebbe utilizzare molteplici fonti di *intelligence* per fornire una valutazione quanto più accurata e aggiornata possibile.

Per ulteriori dettagli sul ruolo del TIP si rimanda al par. 3.6 e al cap. 7 del *framework* TIBER-EU.

2.2.4 *Red Team Tester* (RTT)

Il *Red Team Tester* (RTT) pianifica, sviluppa ed esegue degli scenari di attacco sulle persone, processi, sistemi e servizi inclusi nel perimetro del test. Il suo obiettivo è quello di tentare di violare i presìdi di sicurezza dell'entità testata, seguendo una metodologia di *red teaming* rigorosa ed etica e operando sempre entro i confini della presente Guida e del *framework* TIBER-EU. Le regole di ingaggio e i requisiti specifici per il test sono stabiliti dall'RTT e dall'entità testata.

Per ulteriori dettagli sul ruolo dell'RTT si rimanda al par. 3.6 e ai cap. 8 e 9 del *framework* TIBER-EU.

L'RTT è generalmente un fornitore esterno, in ragione del possibile apporto di una prospettiva più indipendente rispetto a personale interno, nonché della possibilità di disporre di maggiori risorse e competenze più aggiornate. In tal caso i servizi sono stati acquisiti dal CT in linea con gli standard e i requisiti minimi stabiliti nel documento TIBER-EU *Guidance for Service Provider Procurement*. In accordo con il TM, l'RTT può essere interno all'entità testata, attenendosi agli stessi standard e requisiti degli RTT esterni, oltre quanto rappresentato nel par. 3.6.3 del *framework* TIBER-EU.

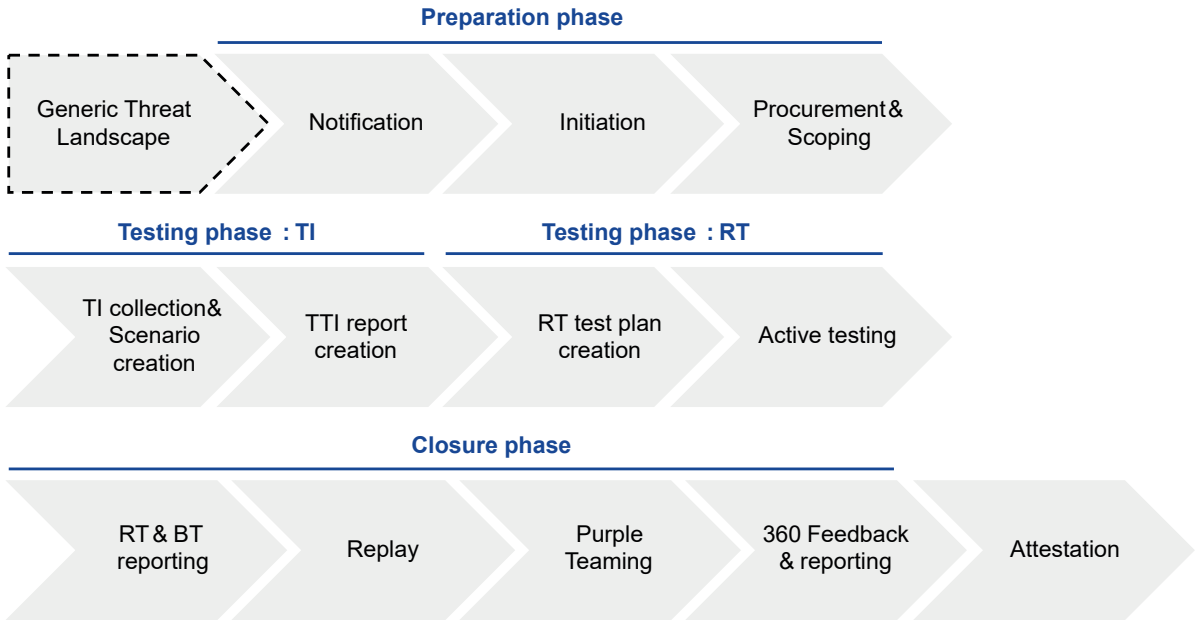
3 PANORAMICA DI ALTO LIVELLO DEL PROCESSO TIBER-IT

nonché delle riunioni previste si rimanda a quanto specificato nel TIBER-EU e nei relativi documenti accessori e, nel caso di TLPT obbligatori, nell'RTS sui TLPT.

3.1 PANORAMICA DEL PROCESSO TIBER-IT E FASI PRINCIPALI

Il processo generale di un test TIBER-IT è composto da tre fasi principali[25]: i) preparazione (*preparation*), ii) *testing* e iii) chiusura (*closure*). Tale processo è completamente allineato a quello descritto nel *framework* TIBER-EU (Figura 1).

Figura 1: PANORAMICA DEL PROCESSO TIBER-IT – PRINCIPALI FASI E ATTIVITÀ (FONTE BCE)



La fase di *preparation* inizia con la notifica (*notification*) con cui l'Autorità TIBER ufficializza l'avvio del test, attraverso una comunicazione trasmessa al punto di contatto designato dall'entità da testare (*written notification*). Successivamente l'entità testata tramite il CT produce i documenti e le informazioni preliminari all'avvio del progetto (*initiation*), identifica il perimetro del test e i relativi obiettivi (*scoping*), acquisisce i servizi esterni (*procurement*) di analisi della minaccia e, se del caso, di *red teaming*. La fase di *preparation* si conclude entro sei mesi dalla ricezione della *written notification*.

La fase di *testing* inizia con l'analisi della minaccia (*threat intelligence*) da parte del TIP e la conseguente creazione di scenari di minaccia specifici per l'entità testata (*TI collection & scenario creation*). Entro un periodo compreso

[25] La creazione e fornitura da parte dell'Autorità TIBER di un panorama della minaccia generico (GTL- *Generic Threat Landscape*) per il settore finanziario italiano è opzionale.

tra 4 e 6 settimane, il TIP finalizza il *Targeted Threat Intelligence Report* (TTIR). Successivamente, la fase di *testing* entra nel periodo di attacco (*red teaming*), in cui l'RTT, indicativamente nelle prime 2 o 3 settimane, sviluppa un piano dettagliato di simulazione dell'attacco (RT *test plan creation*) e in seguito lo esegue (*active testing*) per almeno 12 settimane.

Nella fase di chiusura (*closure*), l'entità testata e l'RTT producono, per quanto di competenza, i report conclusivi del progetto: il *Red Team Test Report* (RTTR), entro quattro settimane dalla chiusura della fase di testing; il *Blue Team Test Report* (BTTR), entro dieci settimane dalla chiusura della fase di testing; il *Test Summary Report* (TSR) e il *Remediation Plan* (RP), entro otto settimane dall'approvazione dei report precedenti. Inoltre, entro dieci settimane dalla chiusura della fase di testing il BT e l'RTT collaborano nella fase di *Purple Teaming* (PT).

La documentazione prodotta dai vari attori durante l'esecuzione di un test TIBER-IT è prioritariamente basata sui modelli del TIBER-EU, fermo restando che, ove ritenuto necessario, può essere personalizzata dall'Autorità TIBER per tener conto delle specificità nazionali. La documentazione è disponibile rispettivamente sul sito Internet della BCE[26] e sul sito Internet della Banca d'Italia dedicato al TIBER-IT[27].

Nelle varie fasi del processo sono previste diverse riunioni formali tra gli attori coinvolti nel test. Con l'accordo tra il TM e il CTL, alcune di tali riunioni potranno essere svolte congiuntamente; inoltre, ne potranno essere previste altre di taglio più operativo o come momenti di confronto.

Ove non esplicitamente specificato, le concrete modalità con cui l'entità testata dovrà inviare la documentazione prevista in ogni fase del processo saranno caso per caso comunicate dal TM.

3.2 Gestione dei rischi durante l'esecuzione del test (risk management)

Il test è condotto su persone, sistemi e servizi che supportano le funzioni critiche dell'entità testata in ambiente di produzione e operativo. Poiché l'esecuzione del test comporta potenziali rischi, il CT deve prevedere adeguati controlli per garantire che il test non infici la corretta operatività dell'entità testata, dei suoi clienti e che non abbia impatti sulla stabilità finanziaria nel suo complesso. L'entità che si sottopone al test è la responsabile del test stesso.

Per tali motivi, il CT deve condurre un'adeguata analisi dei rischi specifici del test e può interrompere il test in qualsiasi momento, dandone comunicazione al TM, se ritiene che la sua continuazione comporti un rischio inaccettabile per l'entità testata. L'analisi del rischio e il correlato piano di gestione devono essere aggiornati nel continuo a fronte di cambiamenti negli scenari e di

---

26 Cfr. https://www.ecb.europa.eu/paym/cyber-resilience/tiber-eu/html/index.en.html.

27 La sezione TIBER-IT è raggiungibile sul sito della Banca d'Italia al seguente percorso: Home/Compiti/Sorveglianza sui mercati e sul sistema dei pagamenti/TIBER-IT: https://www.bancaditalia.it/compiti/sispaga-mercati/tiber-it/index.html.

qualunque altro elemento che possa comportare una modifica nel profilo di rischio connesso all'attività in corso.

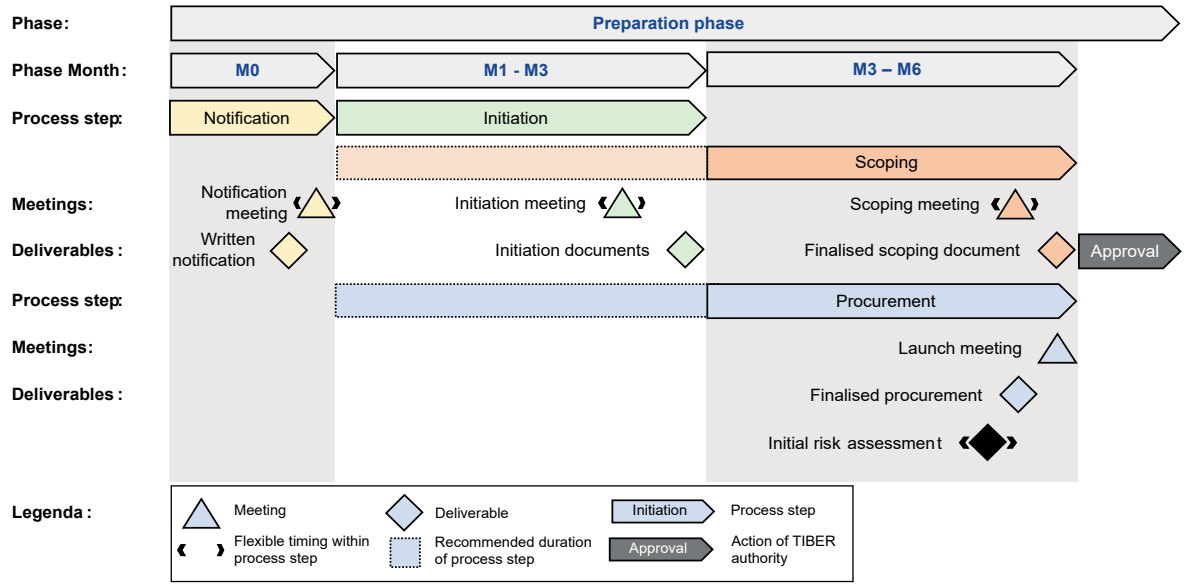
Le funzioni e i sistemi informativi oggetto del test contengono, di norma, informazioni protette ai sensi di legge, quali ad es. informazioni bancarie riservate, comunicazioni elettroniche e dati personali. Pertanto, per tutta la durata del test, dovranno essere assicurati il pieno rispetto della normativa vigente e l'integrità, la disponibilità e la riservatezza delle suddette informazioni attraverso il ricorso a adeguati strumenti di gestione del rischio.

Per ulteriori dettagli sulla gestione del rischio si rimanda al cap. 4 del *framework* TIBER-EU.

4 FASE DI PREPARAZIONE (*PREPARATION*)

La fase di preparazione (*preparation phase*) è composta da quattro step (Figura 2): 1) notifica (*notification*), 2) avvio (*initiation*), 3) identificazione del perimetro del test (*scoping*), e 4) acquisizione dei servizi (*procurement*).

Figura 2: PANORAMICA DEL PROCESSO TIBER-IT – FASE DI PREPARAZIONE



Alcune di queste attività possono essere condotte in parallelo o avviate prima della notifica (ad es. l'acquisizione dei servizi).

In questa Guida è descritta brevemente ogni attività della *preparation phase*. Per ulteriori dettagli si rinvia a quanto previsto nel *framework* TIBER-EU, in particolare al cap. 6.

4.1 NOTIFICA (*NOTIFICATION*)

L'Autorità TIBER invia una comunicazione (*written notification*) al punto di contatto designato dell'entità testata. Tale notifica indica l'inizio della fase di *preparation*, che ha una durata di massimo sei mesi, nonché del test stesso.

Dopo la notifica, il TM organizza un incontro (*notification meeting*) con l'entità testata per illustrare le principali caratteristiche del test, con particolare riferimento ai ruoli, alle responsabilità e alle modalità del test.

4.2 AVVIO (*INITIATION*)

Nello step di avvio (*initiation*), l'entità testata redige i documenti iniziali necessari per l'avvio del test (*initiation documents* - IDs), che devono includere tra l'altro: i) una pianificazione di alto livello del progetto; ii) il nome in codice per il test; iii) i canali di comunicazione da utilizzare; iv) i riferimenti del CTL; v) informazioni di alto livello sulle FEI supportate da terze parti e/o erogate da o verso altre giurisdizioni.

I documenti di avvio sono inviati al TM e presentati dal CTL nel corso della riunione di avvio (*initiation meeting*) entro tre mesi dalla ricezione della notifica iniziale.

Per maggiori informazioni sul contenuto degli *initiation documents* si rinvia alla TIBER-EU *Initiation Documents Guidance*.

4.3 Identificazione del perimetro del test (*scoping*)

In questa fase, l'entità testata deve identificare il perimetro del test, in termini di FEI con le relative persone, sistemi e servizi che le supportano. In linea con le pratiche di gestione del rischio operativo, l'entità testata può condurre o comunque basarsi su una *Business Impact Analysis* (BIA) per stabilire le FEI da testare.

In tale fase devono essere anche definiti gli obiettivi (*flags*) da raggiungere. Tali *flags* possono tuttavia essere modificate su base iterativa durante il test, in seguito alla raccolta di TI e all'evoluzione del test stesso e in accordo con il TM; in questi casi anche il piano di valutazione del rischio (cfr. §3.2) dovrebbe essere aggiornato.

L'esito di questa attività è la definizione dello *Scope Specification Document* (SSD), che è oggetto di confronto con il TM in una riunione dedicata (*scoping meeting*), insieme alla presentazione delle misure di mitigazione dei rischi e della relativa documentazione.

Il TM consulta l'Autorità competente per verificare che i servizi e le funzioni aziendali considerate critiche e/o di particolare interesse dalla stessa siano incluse nel perimetro del test e per eventuali osservazioni sugli obiettivi da raggiungere.

Il documento SSD finalizzato, e approvato da parte del Consiglio di Amministrazione dell'entità testata[28], deve essere inviato al TM, per la validazione da parte dell'Autorità TIBER, entro sei mesi dalla notifica iniziale.

Per maggiori informazioni sul contenuto dello SSD si rinvia alla TIBER-EU *Scope Specification Document Guidance*.

4.4 Acquisizione dei servizi (*procurement*)

Considerando il livello di rischio delle attività di testing condotte in produzione e su sistemi attivi, nonché i dati sensibili gestiti dalle entità che si sottopongono al test, è fondamentale che il TIP e il RTT possiedano i più alti livelli di competenze, capacità e qualifiche in materia. Pertanto, l'entità testata, tramite il CT, ha la responsabilità di selezionare con un rigoroso processo di *due diligence* un TIP esterno e un RTT (interno o esterno) e di verificarne l'adeguatezza secondo la TIBER-EU *Guidance for Service Provider Procurement* e di fornirne l'evidenza al TM.

---

28 Oppure da altro Comitato o personale formalmente incaricato di seguire le attività connesse con i test e per i raccordi con le Autorità.

5 Fase di testing

La fase di test (*testing*) inizia dopo l'approvazione dello SSD, una volta che il TIP e l'RTT sono stati individuati e tutte le attività della fase di preparazione si sono concluse. Si articola in due sottofasi: analisi della minaccia e *red teaming*.

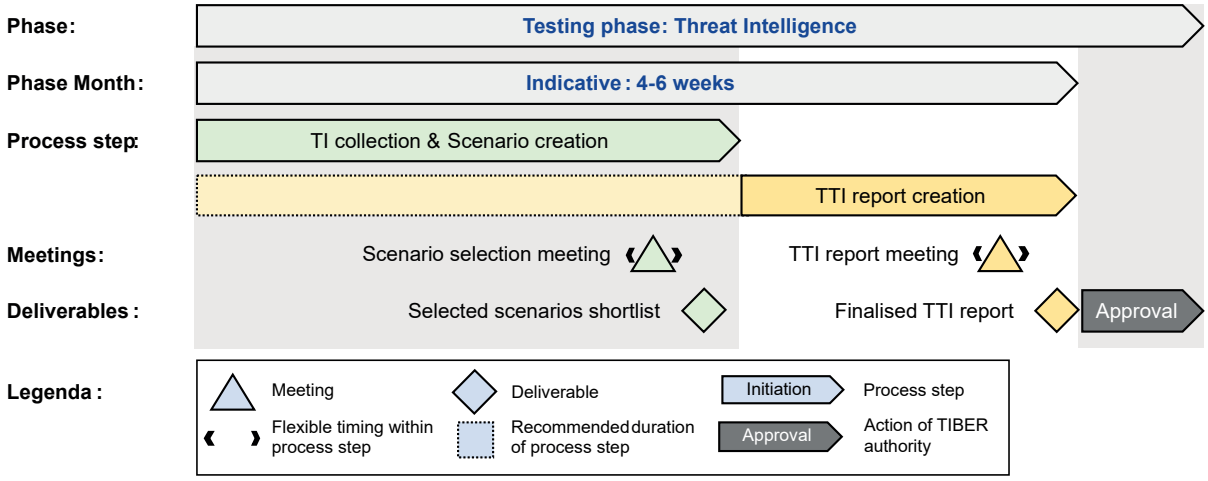
In questa Guida è descritta brevemente ognuna delle due sottofasi. Per ulteriori dettagli si rinvia a quanto previsto nel *framework* TIBER-EU, in particolare ai cap. 7 e 8.

In qualsiasi circostanza è vietato al TIP e all'RTT l'utilizzo in qualsiasi altro contesto al di fuori del test di qualunque informazione sui rischi, sulle minacce e sulle vulnerabilità individuate, sia singolarmente sia in maniera aggregata.

5.1 Analisi della minaccia (*threat intelligence*) e identificazione degli scenari

La sottofase di analisi della minaccia è svolta dal TIP e dura in totale tra le 4 e le 6 settimane (Figura 3). Sulla base dell'analisi del contesto della minaccia cibernetica all'interno del quale si trova ad operare l'entità testata (eventualmente utilizzando uno o più GTL *Report*) e delle informazioni di dettaglio reperibili su di essa (*TI collection*), il TIP[29] sviluppa vari scenari di attacco cyber da parte di attori della minaccia reali (*scenario creation*) specifici per l'entità testata e per le FEI identificate. Tali scenari sono presentati durante una riunione dedicata (*scenario selection meeting*).

Figura 3: PANORAMICA DELLA FASE DI TESTING – *THREAT INTELLIGENCE* (FONTE BCE)



Successivamente, il TIP redige un documento che racchiude le analisi condotte, le relative risultanze, gli scenari proposti e quelli selezionati (*Targeted Threat*

[29] Il TIP deve sempre dimostrare un comportamento profondamente etico e le attività di TTI devono sempre essere condotte nel rispetto delle leggi applicabili.

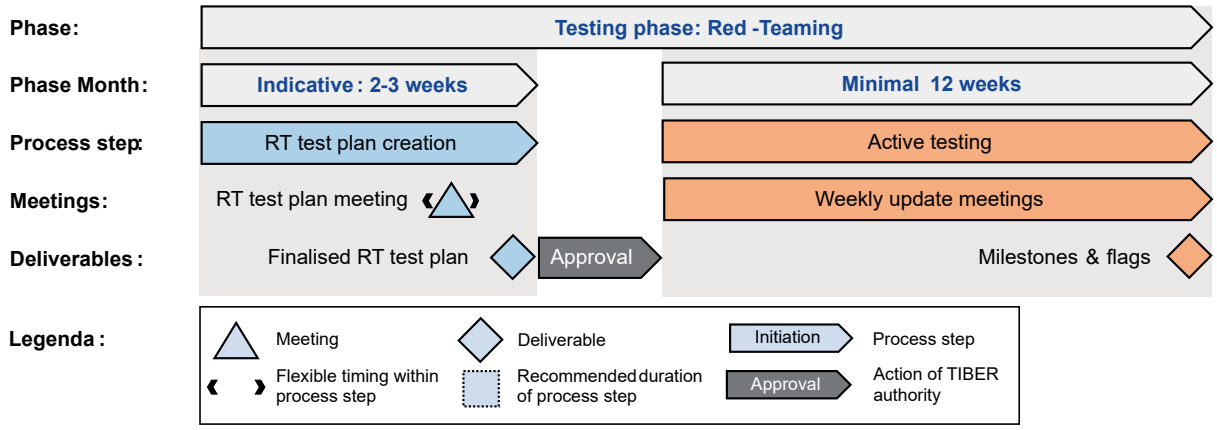
Intelligence Report – TTIR). Per maggiori informazioni sul contenuto del TTIR si rinvia alla TIBER-EU *Targeted Threat Intelligence Report Guidance*.

Il TTIR è oggetto di confronto con il CT e il TM durante una riunione dedicata (*TTI report meeting*) e sucessivamente, per il tramite del CT, sottoposto all'approvazione del TM., il quale verifica la conformità del documento rispetto a quanto previsto dal TIBER-EU.

5.2 Fase di testing: *red teaming*

La fase di testing prosegue con la sottofase di *red teaming*, a sua volta suddivisa in due attività (Figura 4): i) sviluppo del piano di test (*red team test plan creation*) e ii) esecuzione dell'attacco (*active testing*).

Figura 4: PANORAMICA DELLA FASE DI TESTING – *RED TEAMING* (FONTE BCE)



5.2.1 Pianificazione dell'attacco (*red team test plan creation*)

In questa attività, che dura indicativamente tra le 2 e le 3 settimane, l'RTT dettaglia gli scenari di attacco selezionati in precedenza e definisce un piano per ognuno, includendo tra l'altro: tempistiche, sequenza di azioni da simulare (la cosiddetta *kill-chain*), le TTPs che saranno utilizzate, le *flags* che proveranno ad essere raggiunte, i *leg-ups*[30] che potranno essere richiesti. L'RTT presenta al CT e al TM il piano complessivo (*Red Team Test Plan* - RTTP), che deve includere indicazioni anche sulla gestione dei rischi, in una riunione dedicata (*RT test plan meeting*). Per ulteriori dettagli si rinvia a quanto previsto nel *framework* TIBER-EU, in particolare al par. 8.3, e per maggiori informazioni sul contenuto del RTTP alla TIBER-EU *Red Team Test Plan Guidance*. Una volta finalizzato, l'RTTP è approvato prima dal CT e poi dal TM il quale verifica la conformità del documento rispetto a quanto previsto dal TIBER-EU.

[30] Si tratta di informazioni aggiuntive e/o accessi diretti ai sistemi e alla rete, ad esempio tramite credenziali ad hoc, che il CT può fornire all'RTT.

5.2.2 Esecuzione dell'attacco (*active testing*)

Questa attività deve consentire all'RTT[31] di avere il tempo sufficiente per condurre un test realistico e completo, in cui vengono eseguite tutte le fasi di attacco e vengono raggiunti, se possibile, tutti gli obiettivi del test. Il tempo assegnato al test dovrebbe essere proporzionato al perimetro di applicazione, alle risorse dell'entità testata e agli scenari di attaccato previsti nell'RTTP. Comunque, l'esecuzione dell'attacco deve durare almeno 12 settimane.

L'RTT può deviare dagli scenari di attacco previsti all'interno dell'RTTP, in quanto è un'attività che necessita di creatività (come nei reali attacchi cyber), specialmente in caso di eventuali ostacoli e al fine di sviluppare modi alternativi per raggiungere gli obiettivi del test.

Durante l'attacco, l'RTT potrebbe non essere in grado di passare agli step successivi, a causa di vincoli di tempo o perché il BT è riuscito a proteggere adeguatamente l'entità testata. In tali casi, il CT e il TM possono concordare di fornirgli un aiuto per continuare il test (*leg-up*). L'esperienza mostra che esiste una correlazione diretta tra la pertinenza delle informazioni aggiuntive che il CT fornisce all'RTT e il benefit complessivo che l'entità testata trarrà dal test. Tutti gli aiuti devono essere debitamente documentati e riportati nel *Red Team Test Report*.

Durante la fase di test, il CT e l'RTT devono provvedere ad un regolare monitoraggio dei progressi del test, ad esempio tramite comunicazioni e/o incontri giornalieri tramite i canali opportunamente concordati, per aggiornamenti rilevanti quali il raggiungimento di una *flag*, l'individuazione di vulnerabilità potenzialmente critiche, problemi di sicurezza e altri eventi che possano mettere a repentaglio la prosecuzione del test (o parte di esso) o la confidenzialità, integrità e disponibilità dei sistemi aziendali. Inoltre, almeno settimanalmente (*weekly meeting*) il CT e l'RTT aggiornano il TM.

Nel caso le attività dell'RTT siano individuate (*detection*) dal BT e il CT non abbia la possibilità di mantenere la confidenzialità del test (o del singolo scenario), in accordo con il TM, è possibile proseguire in modalità *Purple Teaming* (PT).

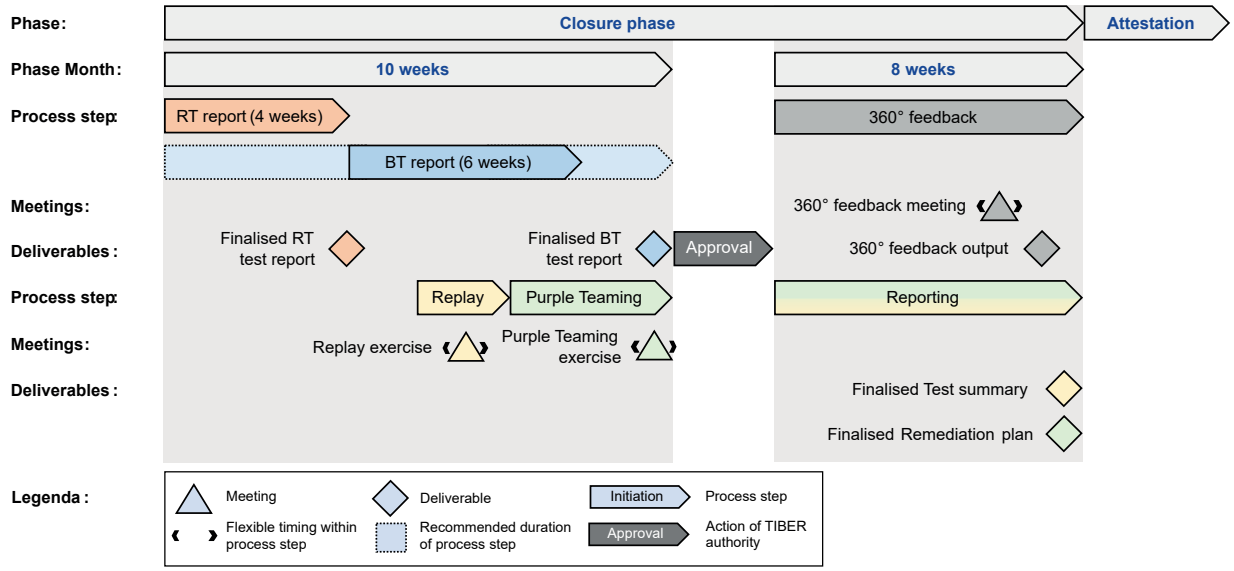
Per ulteriori dettagli si rinvia a quanto previsto nel *framework* TIBER-EU, in particolare al par. 8.4, e per maggiori informazioni sul PT alla TIBER-EU *Purple Teaming Guidance*.

6 Fase di chiusura (*closure*)

La fase di chiusura (*closure phase*) inizia al termine dell'esecuzione dell'attacco ed è dedicata all'analisi delle attività svolte durante il test insieme al BT, che è ormai stato informato del test, e a pianificare i dovuti miglioramenti per rafforzare la resilienza cyber dell'entità sottoposta a test (Figura 5).

[31] L'RTT deve sempre dimostrare un comportamento profondamente etico e le attività devono sempre essere condotte nel rispetto delle leggi applicabili.

Figura 5: PANORAMICA DELLA FASE DI CHIUSURA (FONTE BCE)



Il test si conclude con il rilascio dell'attestazione. Il successivo, eventuale, monitoraggio del piano di rimedio è responsabilità dell'Autorità competente, nell'ambito delle ordindarie attività di supervisione.

Per ulteriori dettagli si rinvia a quanto previsto nel *framework* TIBER-EU, in particolare al cap. 9.

6.1 Report del Red Team, del Blue Team e riproduzione dell'attacco

Nel primo step della fase di chiusura, che dura al massimo dieci settimane, sono svolte diverse attività di *reporting* tecnico e di riproduzione di quanto successo durante il test:

- redazione del *Red Team Test Report*;
- redazione del BT *Report*;
- l'esecuzione del *Replay Exercise;*
- svolgimento del *Purple Teaming*.

Entro quattro settimane dalla fine della fase di attacco l'RTT invia al CT e al TM un documento (RTTR) che riepiloga in dettaglio, tra l'altro, tutte le attività svolte durante l'attacco, con relativa *timeline*, gli obiettivi raggiunti, le TTPs utilizzate con successo, le vulnerabilità riscontrate, le possibili cause (*root causes*) e le relative raccomandazioni per una loro correzione.

Per maggiori informazioni sul contenuto dell'RTTR si rinvia alla TIBER-EU *Red Team Test Report Guidance*.

Il BT utilizza l'RTTR, eventualmente anche in una versione non ancora finalizzata, per predisporre un documento (BTTR) che include i dettagli delle attività eseguite o non eseguite dal BT stesso durante la fase di attacco a seguito

delle azioni dell'RT (ad es., analisi dei log e degli allarmi generati, misure di contentimento e mitigazione, etc). Il BTTR è finalizzato e inviato al CT e al TM entro dieci settimane dalla fine della fase di attacco.

Per maggiori informazioni sul contenuto del BTTR si rinvia alla TIBER-EU *Blue Team Test Report Guidance*.

Il BTTR, eventualmente anche in una versione non ancora finalizzata, è utilizzato, insieme all'RTTR, durante il *Replay Exercise*, in cui l'RTT e il BT ripercorrono congiuntamente gli scenari di attacco svolti, seguendo la relativa sequenza temporale delle principali attività condotte da ciascun team, con l'obiettivo di confrontarsi a livello tecnico su quanto eseguito e sulle contromisure utilizzate o possibili. Infine, l'RTT e il BT collaborano anche in un esercizio di PT, in cui sono analizzate, ad esempio, ulteriori attività che potevano essere eseguite dall'RTT, ma che per mancanza di tempo o perché troppo rischiose non sono state svolte, e/o TTPs che potevano essere utilizzate durante il test.

Per maggiori informazioni sull'esercizio di PT si rinvia alla TIBER-EU *Purple Teaming Guidance*.

6.2 Report di sintesi (*test summary report*) e piano di rimedio (*remediation plan*)

Nel secondo step della fase di chiusura, dopo che l'RTTR e il BTTR sono stati finalizzati, l'entità testata, sulla base di tutta la documentazione prodotta durante il test, ricapitola in un documento di sintesi (TSR) il complessivo processo di test e i relativi risultati.

Per maggiori informazioni sul contenuto del TSR si rinvia alla TIBER-EU *Test Summary Report Guidance*.

In parallelo, sulla base delle raccomandazioni prodotte dall'RTT e dal BT, l'entità testata produce un piano di rimedio (RP), con l'obiettivo di sanare le vulnerabilità (e le cause ad esse connesse) riscontrate durante il test. l'RP non dovrebbe includere solamente azioni di rimedio puramente tecniche ma, ove necessario, anche azioni a più ampio spettro, volte a migliorare i processi interni dell'entità testata.

Per maggiori informazioni sul contenuto dell'RP si rinvia alla TIBER-EU *Remediation Plan Guidance*.

Il TM consulta l'Autorità competente per eventuali osservazioni sul TSR e sul relativo RP predisposti dall'entità testata.

Entro otto settimane dalla finalizzazione dell'RTTR e del BTTR, l'entità testata invia al TM la versione definitiva del TSR e dell'RP, quest'ultimo viene inviato anche all'Autorità competente se diversa dall'Autorità TIBER.

Prima della conclusione effettiva del test, il TM organizza un incontro per raccogliere i *feedback* dagli attori coinvolti nel processo di test (*360-degree Feedback Meeting*), con l'obiettivo di analizzare congiuntamente il test e i possibili aspetti da migliorare nell'approccio seguito, in caso di ulteriori test futuri, e nella metodologia TIBER-IT nel suo complesso.

6.3 Attestazione

Al termine della fase di chiusura, una volta che l'Autorità TIBER ha valutato il rispetto dei requisiti applicabili per il processo di test nel suo complesso e approvato il TSR e l'RP, viene rilasciata un'attestazione[32] all'entità testata in cui si conferma che il processo di test si è concluso ed è stato condotto conformemente ai requisiti dettagliati nella presente Guida e, nel caso di TLPT obbligatori, a quantoprescritto da DORA e dall'RTS sui TLPT. L'Autorità TIBER non esprime alcuna valutazione sui risultati emersi dal test, che per sua natura non è di tipo "*pass or fail*".

L'attestazione può essere utilizzata dall'entità testata per l'eventuale mutuo riconoscimento del test da parte di altre autorità nazionali o di altri Paesi.

Per maggiori informazioni sul contenuto dell'attestazione si rinvia alla TIBER-EU *Attestation Guidance*.

[32] Fatti salvi eventuali accordi tra le Autorità competenti in relazione alla responsabilità di rilascio e comunicazione dell'attestazione nel caso di utilizzo delle deleghe previste ai sensi di DORA.

7 INTERAZIONI E FLUSSI DI COMUNICAZIONE DURANTE UN TEST TIBER-IT

Durante tutte le fasi dei test TIBER-IT sono assicurate continue e strette interazioni tra tutti i principali *stakeholders*.

Nella presente Guida sono state descritte tutte le interazioni tra CT e TCT/TM, così come la stretta cooperazione tra il TIP e l'RTT. Inoltre, se ritenuto necessario e in base alle caratteristiche dell'entità sottoposta a test, il TM può interagire anche con altre autorità finanziarie nazionali e internazionali e agenzie di cyber sicurezza governative.

Tutte le parti coinvolte in un test TIBER-IT adottano un approccio collaborativo, trasparente e flessibile al test. Ciò non vale per il BT, che deve rimanere ignaro del test fino alla fase di chiusura.

Il modo in cui si svolgono le comunicazioni è concordato tra le parti interessate, al fine di proteggere la riservatezza delle informazioni scambiate. Per le stesse ragioni, il nome in codice dell'entità sottoposta a test è utilizzato per tutta la durata del test stesso. Per proteggere ulteriormente la riservatezza dei dati e delle informazioni, ove opportuno, il TIP e l'RTT dovrebbero firmare un accordo di riservatezza (NDA) con l'entità sottoposta a test.

Eventuali significative deviazioni dalla pianificazione iniziale sono discusse con il TM. È fondamentale che in ogni fase tutte le parti interessate si tengano informate a vicenda per garantire che il test proceda senza impedimenti e che eventuali problemi (ad es. vincoli di risorse o difficoltà logistiche e operative) possano essere affrontati tempestivamente.

Al fine di migliorare non solo la resilienza dell'entità sottoposta a test, ma quella dell'intero settore finanziario, il TCT può analizzare i risultati di alto livello di tutti i test (ad es. il *Test Summary Report*) per identificare le principali problematiche, le aree tematiche, le minacce e le vulnerabilità comuni, e diffonderli in forma anonimizzata alle parti interessate.

8 Indice delle figure

9 Allegati

9.1 Allegato I: lista degli acronimi

Tabella 1: LISTA DEGLI ACRONIMI

Acronimo	Descrizione
BIA	*Business Impact Analysis*
BT	*Blue Team*
BTTR	*Blue Team Test Report*
CAP	*Codice delle Assicurazioni Private (d.lgs. 209/2005)*
CERTFin	*Computer Emergency Response Team* per il settore finanziario italiano
CIISI-EU	*Pan-european Cyber Information and Intelligence Sharing Initiative*
CT	*Control Team*
CTL	*Control Team Lead*
DORA	*Regolamento (UE) 2022/2554 del Parlamento Europeo e del Consiglio del 14 dicembre 2022 relativo alla resilienza operativa digitale per il settore finanziario e che modifica i regolamenti (CE) n. 1060/2009, (UE) n. 648/2012, (UE) n. 600/2014, (UE) n. 909/2014 e (UE) 2016/1011*
ECRB	*Euro Cyber Resilience Board for pan-European Financial Infrastructures*
FC o FEI	*Funzioni Critiche* o *Funzioni Essenziali o Importanti*
GTL	*Generic Threat Landscape*
ID	*Initiation Documents*
NDA	*Accordo di riservatezza (Non-Disclosure Agreement)*
PT	*Purple Teaming*
RP	*Remediation Plan*
RTS sui TLPT	*Regolamento delegato (ue) 2025/1190 della Commissione del 13 febbraio 2025 che integra il regolamento (UE) 2022/2554 del Parlamento europeo e del Consiglio per quanto riguarda le norme tecniche di regolamentazione che specificano i criteri utilizzati per identificare le entità finanziarie che hanno l'obbligo di svolgere test di penetrazione guidati dalla minaccia, i requisiti e le norme che disciplinano il ricorso a soggetti incaricati dello svolgimento dei test interni, i requisiti concernenti l'ambito, l'approccio e la metodologia da seguire per i test in ciascuna fase dei test, i risultati, la chiusura e le fasi correttive e il tipo di cooperazione di vigilanza e altri tipi di cooperazione pertinenti necessari per svolgere i TLPT e per la facilitazione del riconoscimento reciproco*
RTT	*Red Team Tester*
RTTP	*Red Team Test Plan*
RTTR	*Red Team Test Report*
SSD	*Scope Specification Document*

Tabella 1: LISTA DEGLI ACRONIMI

Acronimo	Descrizione
SSM	*Single Supervisory Mechanism*
TCT	*TIBER Cyber Team* o *TLPT Cyber Team*
TI	*Threat Intelligence*
TIBER	*Threat Intelligence-Based Ethical Red Teaming*
TLPT SC	*TLPT Steering Committee for the Italian financial sector - Gruppo di coordinamento sul TLPT per il sistema finanziario italiano*
TIP	*Threat Intelligence Provider*
TKC	TIBER-EU *Knowledge Centre*
TLPT	*Threat-Led Penetration Testing*
TM	*Test Manager*
TSR	*Test Summary Report*
TTIR	*Targeted Threat Intelligence Report*
TTPs	*Tattiche, Tecniche e Procedure (Tactics, Techniques and Procedures)*
TUB	*Testo Unico Bancario (d.lgs. 385/1993)*
TUF	Testo Unico della Finanza (d.lgs. 58/1998)

9.2 Allegato II: ulteriore documentazione e principali riunioni

Per lo svolgimento di un test, tutte le parti interessate si basano su una serie di documenti di accompagnamento che forniscono orientamenti aggiuntivi e più specifici o servono come modelli da utilizzare durante il processo di test.

A meno di eventuali specificità nazionali per le quali il TCT predispone e mette a disposizione documenti e modelli dedicati, si fa riferimento a quanto predisposto in ambito europeo per il *framework* TIBER-EU, di cui alla Tabella 2 di cui sotto.

Nella Tabella 3 sono elencate le principali riunioni previste dalla metodologia.

Ulteriori informazioni possono essere richieste a: tiber-it@bancaditalia.it.

Tabella 2: ULTERIORE DOCUMENTAZIONE DISPONIBILE SUL SITO DELLA BCE

#	Titolo
1	TIBER-EU Framework: How to implement the European framework for Threat Intelligence-Based Ethical Red teaming
2	TIBER-EU Guidance for Service Provider Procurement
3	TIBER-EU Control Team Guidance
4	TIBER-EU Purple Teaming Guidance
5	TIBER-EU Initiation Documents Guidance
6	TIBER-EU Scope Specification Document Guidance
7	TIBER-EU Targeted Threat Intelligence Report Guidance
8	TIBER-EU Red Team Test Plan Guidance
9	TIBER-EU Red Team Test Report Guidance
10	TIBER-EU Blue Team Test Report Guidance
11	TIBER-EU Remediation Plan Guidance
12	TIBER-EU Test Summary Report Guidance
13	TIBER-EU Attestation Guidance

Tabella 3: PRINCIPALI RIUNIONI

#	Lista delle principali riunioni	Parti coinvolte
1	Notification	TM, rappresentanti dell'entità testata (ad es., CTL e/o futuri membri del CT)
2	Initiation	TM, CTL e futuri membri del CT
3	Scoping	CTL, CT, TM, TIP e/o RTT (se già disponibili)
4	Launch	CTL, CT, TM, TIP e RTT
5	Scenario selection	CTL, CT, TM, TIP e RTT
6	Targeted threat intelligence	CTL, CT, TM, TIP e RTT
7	Red Team Test Plan	CTL, CT, TM, RTT e TIP (se necessario)
8	Riunioni settimanali o aggiornamenti sul test	CTL, CT, TM, RTT e TIP (se necessario)
9	Replay Exercise	CTL, CT, BT, RTT e TM (se necessario)
10	PT Exercise	CTL, CT, BT, RTT
11	360-degree Feedback meeting	TM, CTL, CT, BT, TIP, RTT e TCT (se necessario)