CONSOB | Commissione Nazionale per le Società e la Borsa
Autorità italiana per la vigilanza dei mercati finanziari

BANCA D'ITALIA
EUROSISTEMA

IVASS
Istituto per la Vigilanza sulle Assicurazioni

Guida nazionale TIBER-IT

Threat Intelligence Based Ethical Red-Teaming – Italia

Agosto 2022 - versione 1.0

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

Negli ultimi anni la resilienza cyber è diventata una priorità internazionale a seguito della crescente digitalizzazione e interconnessione dei servizi finanziari, con il conseguente aumento della sofisticazione e persistenza dei rischi cyber.

Per affrontare i crescenti rischi cyber, le Autorità finanziarie hanno compiuto passi significativi per il rafforzamento della resilienza cyber delle entità finanziarie e del settore nel suo complesso.

Nel 2016 il G-7 ha pubblicato i "*Fundamental elements for cyber security in the financial sector* (G7FE)" e il CPMI-IOSCO ha pubblicato la "*Guidance of Cyber Resilience for Financial Market Infrastructures*", che riconosce i test, comprese le esercitazioni di tipo *red teaming*, come una componente chiave per mantenere un'adeguata postura di resilienza cyber. Inoltre, il documento del G-7 "*Fundamental Elements for Threat-Led Penetration Testing* (G7FE-TLPT)", pubblicato nel 2018, fornisce orientamenti alle entità finanziarie per valutare, attraverso simulazioni, la loro resilienza a fronte di incidenti cyber malevoli e alle Autorità per considerare di introdurre all'interno delle rispettive giurisdizioni l'utilizzo di *Threat-Led Penetration Testing* (TLPT). Nello stesso anno la BCE ha pubblicato il *framework* TIBER-EU[1].

A livello nazionale e secondo le rispettive competenze, 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. Tale collaborazione si svolge nella cornice di cooperazione internazionale ed europea, ed è condotta attraverso l'attività di supervisione, il dialogo continuo tra autorità e industria nonché attraverso la partecipazione alle principali sedi cooperative pubblico-private nazionali in tema di *cybersecurity*[2].

All'inizio del 2020 la Banca d'Italia e la Consob hanno lanciato un piano d'azione congiunto per rafforzare la resilienza cyber del settore finanziario italiano, attraverso l'applicazione di specifiche misure rivolte ai sistemi di pagamento, alle controparti centrali, ai depositari centrali e alle sedi di negoziazione. Il piano prevede l'adozione di strumenti già sviluppati dall'Eurosistema, tra cui le *Cyber Resilience Oversight Expectations* (CROE) e il TIBER-IT, ossia il recepimento nazionale del *framework* TIBER-EU. Anche i settori bancario e assicurativo mostrano un crescente interesse per l'esecuzione di TLPT, come strumento efficace per migliorare il livello di resilienza cyber degli intermediari. Pertanto, le Autorità di regolamentazione e le Autorità di vigilanza bancarie e assicurative sono impegnate nel recepimento e nell'attuazione del TIBER-IT.

---

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

2 Il ***Computer Emergency Response Team*** per il settore finanziario italiano (CERTFin) e la struttura per il coordinamento delle crisi operative della piazza finanziaria italiana (Codise).

Come recepimento del *framework* TIBER-EU, la presente Guida nazionale TIBER-IT offre una metodologia e un modello operativo che possono essere adottati su base volontaria dalle entità finanziarie e dalle imprese di assicurazione per testare e migliorare le proprie capacità di protezione, rilevamento e risposta rispetto agli incidenti cyber malevoli.

Durante tutto il processo, i test TIBER-IT prevedono un forte coinvolgimento di tutti i portatori di interesse (approccio *multi-stakeholder*). Prima dell'inizio formale di un test, le entità identificano principali parti interessate e si impegnano adeguatamente con esse, comprese le Autorità pertinenti.

In conformità con il *framework* TIBER-EU, l'impegno delle parti interessate mira inoltre a supportare, specie nel caso di entità con operatività in più Paesi e coinvolte in valutazioni che riguardano più giurisdizioni, test TIBER-IT di tipo transfrontaliero, anche al fine di promuovere un adeguato dibattito relativo al reciproco riconoscimento dei risultati dei test TIBER-IT e di migliorare i protocolli per la condivisione dei relativi risultati, facendo anche leva sul TIBER-EU *Knowledge Centre* (TKC) istituito presso la BCE[3].

Poiché i test TIBER-IT sono molto intrusivi e delicati, tutte le parti interessate, il management aziendale e in particolare il *White Team* (WT, cfr. §3.2.3) devono attribuire la massima priorità alla chiara definizione del perimetro di applicazione (*scope*) del test e all'applicazione di controlli efficaci per la gestione dei rischi per tutta la durata del processo.

Tramite l'esecuzione di test TIBER-IT, le entità finanziarie favoriscono fortemente la propria resilienza operativa; le Autorità finanziarie ottengono, ai fini della stabilità finanziaria, un'adeguata assicurazione relativa alla postura di resilienza cyber sia a livello di singola entità che settoriale, ove il *framework* sia adottato dai principali operatori.

In questo contesto la Banca d'Italia, coerentemente con il suo mandato di assicurare stabilità monetaria e finanziaria, riveste ai fini della Guida nazionale il ruolo di Autorità capofila del TIBER-IT (la cosiddetta TIBER-IT *Lead Authority*) e ne cura i compiti in stretta collaborazione con Consob e IVASS. La manutenzione del TIBER-IT e il suo allineamento con il TIBER-EU e altre pertinenti migliori pratiche internazionali sono guidati da un Gruppo di coordinamento interistituzionale tra le tre Autorità (TIBER-IT *Steering Committee* – SC, cfr. §3.2.1).

Nel resto del documento:

- con il termine "le Autorità" si intendono la Banca d'Italia, la Consob e l'IVASS;
- il termine "entità finanziarie", se non diversamente specificato, comprende le infrastrutture del mercato finanziario, i sistemi di pagamento e le

[3] Il TKC è un forum composto da rappresentanti delle istituzioni che hanno recepito il ***framework*** TIBER-EU. I suoi obiettivi principali sono: i) manutiene 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.

infrastrutture di supporto tecnologico o di rete[4], le sedi di negoziazione, le banche, gli istituti di pagamento e di moneta elettronica, gli intermediari finanziari ex art. 106 TUB e le imprese di assicurazione nonchè gli intermediari assicurativi[5];

- il termine "settore finanziario" comprende le entità finanziarie sopra descritte.

1.2 Cos'è il TIBER-IT

Il TIBER-IT recepisce a livello nazionale il *framework* TIBER-EU, tenendo conto delle specificità nazionali ed è volto ad assicurare il riconoscimento dei test da parte delle altre giurisdizioni che recepiscono il TIBER-EU. Le Autorità collaborano tra di loro per il recepimento del *framework* TIBER-EU come descritto nella presente Guida.

La Banca d'Italia, in stretta collaborazione con Consob e IVASS, guida ed è responsabile dell'attuazione e dell'aggiornamento di TIBER-IT, la cui compatibilità con altri quadri e metodologie nazionali di TLPT sarà garantita nella massima misura possibile.

Il TIBER-IT simula potenziali attacchi reali riproducendo tattiche, tecniche e procedure (TTP) di attori della minaccia reali, verificando così le capacità di rilevamento, protezione e risposta dell'entità testata.

TIBER-IT è uno strumento volontario, adottato per favorire la stabilità finanziaria e la resilienza cyber; il suo utilizzo non è un requisito di regolamentazione, sorveglianza o vigilanza.

1.3 Profili giuridici

L'opportunità del recepimento del TIBER-EU, con la Guida nazionale TIBER-IT che ne rappresenta la metodologia nazionale, fa perno principalmente sulle competenze attribuite alla Banca d'Italia, e su quelle attribuite a Consob e IVASS, in materia di stabilità complessiva, efficienza e competitività del sistema finanziario italiano[6], nonché di quelle concernenti la sorveglianza sul regolare funzionamento, affidabilità ed efficienza del sistema dei pagamenti[7]. Tali sistemi, infatti, fortemente digitalizzati e interconnessi sono suscettibili di minaccia in conseguenza dell'aumento della sofisticazione e della persistenza dei rischi cyber.

---

4 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).

5 Quest'ultimi ove rilevanti per la distribuzione assicurativa a livello nazionale.

6 Ex 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).

7 Ex art. 146, comma 1, TUB.

Inoltre, in analogia a quanto effettuato in altre giurisdizioni, l'implementazione della metodologia nazionale si basa sulla collaborazione tra le Autorità del settore finanziario nazionale, che comprendono anche la Consob e l'IVASS, nel perseguimento del comune interesse di mantenere la resilienza complessiva del sistema bancario, finanziario e assicurativo italiano. La messa a disposizione della metodologia TIBER-IT e la sua adozione, su base volontaria, da parte delle entità finanziarie contribuisce all'innalzamento della cyber resilience del sistema nel suo complesso.

1.4 Scopo e ambito di applicazione della Guida

La presente Guida mira a migliorare la resilienza delle entità finanziarie e del settore finanziario italiano nel suo complesso, fornendo un approccio comune per assicurare che le funzioni critiche[8] (FC) delle entità finanziarie siano adeguatamente protette da attacchi cyber mirati.

La Guida fornisce una panoramica sulle modalità di recepimento del TIBER-EU in Italia e, in particolare, descrive il processo complessivo e i suoi componenti chiave quali fasi, attività, prodotti e risultati finali, ruoli e responsabilità, nonché le interazioni tra i diversi attori coinvolti in un test TIBER-IT.

Le entità finanziarie, su base volontaria, assumono le determinazioni sulla conduzione dei test e allocano le risorse per pianificare e organizzare i test secondo quanto stabilito dalla presente Guida. Le Autorità forniscono supporto metodologico alle entità finanziarie incluso, se disponibile, il *Generic Threat Landscape*[9] (GTL) del settore finanziario aggiornato.

La Guida è indirizzata alle entità finanziarie e ai loro fornitori di servizi di analisi della minaccia (*threat intelligence* - TI) e *red teaming* (RT).

Per lo svolgimento dei test, oltre che al TIBER-IT le entità finanziarie devono fare riferimento, per quanto nello stesso non dettagliato anche al *framework* TIBER-EU e alla relativa documentazione supplementare di riferimento, secondo quanto tempo per tempo dalla stessa previsto e rilasciata dalla BCE, responsabile del mantenimento del TIBER-EU. A titolo esemplificativo si veda la Figura 1[10].

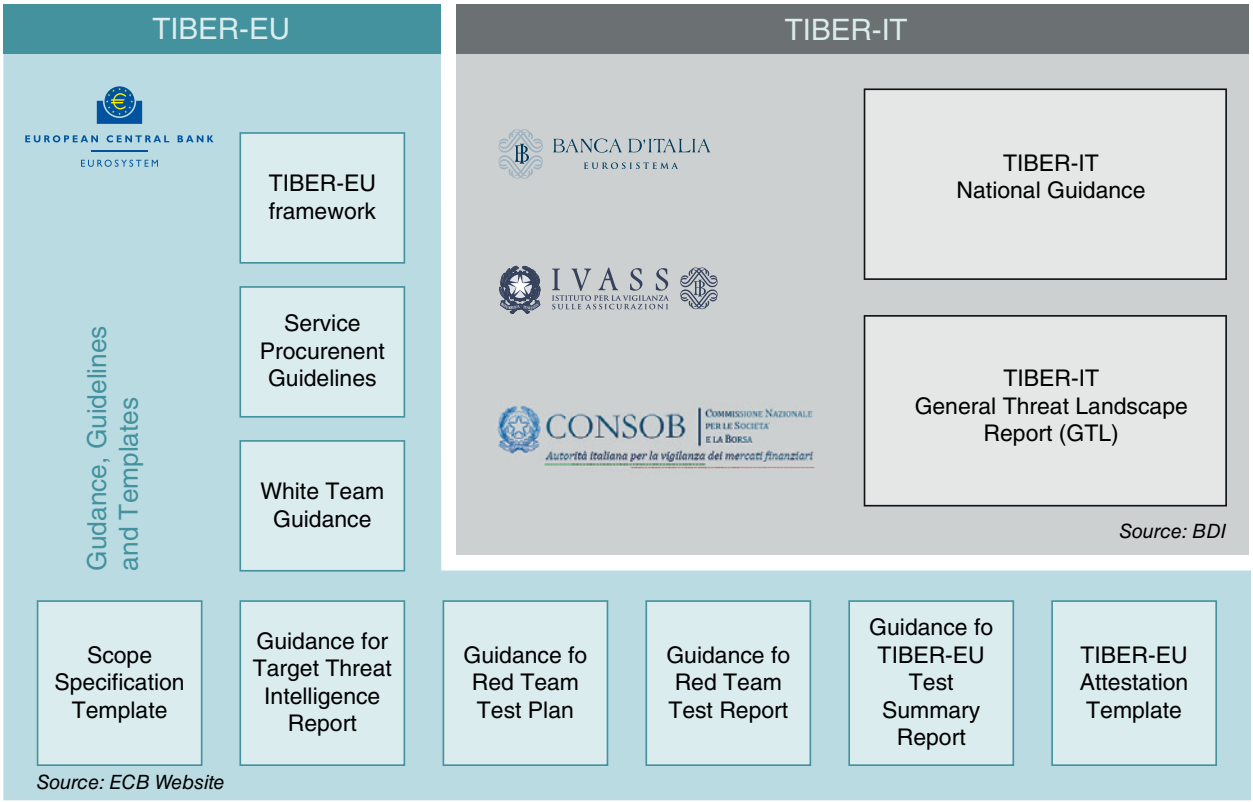
---

8 Nel ***framework*** TIBER-EU le FC sono definite come: "le persone, i processi e le tecnologie necessarie all'entità per fornire un servizio fondamentale che, se interrotto, potrebbe avere un impatto negativo sulla stabilità finanziaria, sulla sicurezza e solidità dell'entità, sui suoi clienti o sulla sua condotta di mercato" (traduzione non ufficiale ai fini della presente Guida).

9 Il GTL è un documento che descrive lo scenario di minaccia generale applicabile al sistema finanziario.

10 Al fine di facilitare il raccordo sia con il ***framework*** TIBER-EU sia con le contestualizzazioni delle altre giurisdizioni, le figure e i nomi dei principali attori, documenti e riunioni sono riportati principalmente in inglese.

Figura 1: DOCUMENTAZIONE DI RIFERIMENTO PER LO SVOLGIMENTO DEI TEST TIBER-IT – DOCUMENTAZIONE E INTERAZIONI CON IL TIBER-EU



1.5 Nota legale e *copyright*

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

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

Le entità finanziarie 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, in relazione al quale la BCE detiene tutti i diritti d'autore, ed è ampiamente allineata con le guide TIBER pubblicate in altri paesi dell'Unione europea, quali ad es. il TIBER-NL, il TIBER-DE, il TIBER-DK, il TIBER-BE, il TIBER-IE, TIBER-FI e nella massima misura possibile, con implementazioni simili in giurisdizioni non europee come il CBEST nel Regno Unito.

2 Recepimento del TIBER-EU e implementazione del TIBER-IT

Il TIBER-EU è formalmente recepito nella giurisdizione italiana dalle Autorità tramite l'implementazione del TIBER-IT. La BCE e i membri del *Tiber Knowledge Centre*[3] (TKC) sono stati ufficialmente informati del recepimento e sono costantemente aggiornati.

Le Autorità promuovono la partecipazione volontaria delle entità finanziarie ai test TIBER-IT, indirizzano la relativa programmazione annuale e pluriennale consultando le entità finanziarie che hanno espresso la loro disponibilità a sottoporsi ai test.

I dettagli delle attività dei test TIBER-IT sono pianificati su base annuale. Al fine di dare alle entità finanziarie la possibilità di includere il test TIBER-IT nella loro pianificazione annuale, il termine per esprimere la disponibilità di sottoporsi al test tiene conto del ciclo annuale di pianficazione e bilancio delle entità finanziarie. Per la partecipazione ai test non è previsto alcun costo da corrispondere alle Autorità.

Le entità finanziarie decidono di sottoporsi ad un test TIBER-IT su base volontaria e stanziano le risorse necessarie, conducono le attività di test e ne riferiscono alle parti coinvolte nel processo, secondo quanto previsto dalla presente Guida. La decisione di partecipare al test dovrebbe essere presa a livello di Consiglio di Amministrazione o di organo analogo dell'entità finanziaria.

Le Autorità forniscono orientamenti e supporto per lo sviluppo del TIBER-IT da parte dell'entità che si sottopone al test. Per lo svolgimento di questi compiti, le Autorità assicurano un *TIBER Cyber Team* (TCT, cfr. 3.2.2) che opera al fine di facilitare l'esecuzione del test e di garantirne il mutuo riconoscimento da parte di altre Autorità rilevanti ove necessario. Il TCT mantiene i contatti con il TKC e con i TCTs di altre Autorità e/o paesi.

Il TCT, con il supporto delle altre parti interessate, inoltre fornisce e mantiene aggiornato il report *Generic Threat Landscape* (GTL) che mira a supportare le entità finanziarie durante la fase di *threat intelligence* del processo di test TIBER-IT.

In aggiunta, le entità che si sottopongono a test acquisiscono i servizi di *threat intelligence* e *red teaming* seguendo le istruzioni presenti nel documento "TIBER-EU *Services Procurement Guidelines*[11]". Il fornitore di *Threat Intelligence* (TI *Provider*) dovrebbe sfruttare, se disponibile, il GTL per consegnare il *Targeted Threat Intelligence* (TTI)[12] Report all'entità finanziaria testata.

Maggiori dettagli sui ruoli e le responsabilità degli attori TIBER-IT possono essere consultati al § 3.2.

---

11 https://www.ecb.europa.eu/pub/pdf/ecb.tiber_eu_services_procurement_guidelines.en.pdf.

12 Il TTI Report fornisce una visione dettagliata sulla superficie di attacco dell'entità e sui suoi presìdi di difesa (cfr. § 3.5.1).

2.1 Ambito di applicazione del TIBER-IT

Il TIBER-IT è adottato con un approccio graduale, ed è prioritatiamente rivolto alle entità finanziarie "critiche" per il sistema finanziario italiano con l'obiettivo di migliorare la loro resilienza cyber e di contenere gli impatti sistemici che un incidente cyber può causare al settore finanziario italiano nel suo complesso.

Nello specifico, il gruppo di riferimento (*target group*) delle entità finanziarie comprende i seguenti soggetti operanti in Italia:

- 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;
- gli intermediari finanziari ex art. 106 TUB;
- imprese di assicurazione;
- intermediari assicurativi[5].

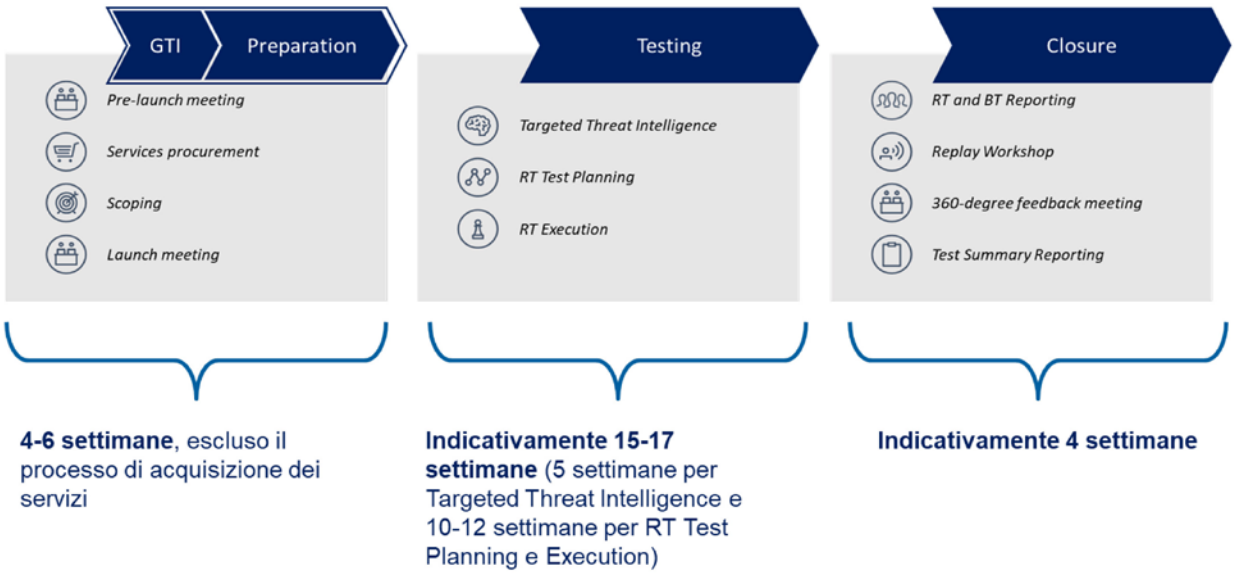
Tuttavia, la definizione del gruppo di riferimento a cui si rivolge principalmente il TIBER-IT non preclude il ricorso ad un approccio flessibile per valutare eventuali test TIBER-IT su un tipo di entità non già incluso nell'elenco o con diverse caratteristiche, tenendo conto ad es. delle sue interconnessioni con altre entità finanziarie e della sua maturità cyber.

3 PANORAMICA DI ALTO LIVELLO DEL PROCESSO TIBER-IT

3.1 PANORAMICA DEL PROCESSO TIBER-IT E FASI PRINCIPALI

Il processo generale di un test TIBER-IT è composto da tre fasi principali (Figura 2): i) preparazione (*preparation*), ii) *testing* e iii) chiusura (*closure*) ed è completamente allineato al processo descritto nel *framework* TIBER-EU.

Figura 2: PANORAMICA DEL PROCESSO TIBER-IT – PRINCIPALI FASI E ATTIVITÀ



La fase di *preparation* inizia con una riunione preliminare (*pre-launch meeting*), a cui segue l'acquisizione dei servizi esterni e l'identificazone del perimetro del test (*scoping)*, e conduce a una riunione di avvio (*launch meeting*).

La fase di *testing* inizia con l'analisi delle minacce e la loro contestualizzazione per il singolo test (*targeted threat intelligence*) seguita dalla pianificazione ed esecuzione delle attività di *red teaming* da parte dei fornitori di servizi, rispettivamente il TI Provider ed il RT Provider.

Dopo il completamento del *red teaming* test, la fase di chiusura inizia con la produzione del RT Report e del *Blue Team* (BT) report, seguita da un *replay workshop*, dalla riunione di feedback (*360-degree feedback meeting*) e dallo sviluppo del report di riepilogo dei test (*Test Summary Report*).

Al fine di favorire nell'UE l'armonizzazione e la standardizzazione dell'approccio ai test di sicurezza avanzati guidati dalla minaccia (*threat intelligence based ethical red-teaming)*, la documentazione prodotta dall'entità testata 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 dalle Autorità per tener conto delle specificità nazionali.

La documentazione è disponibile rispettivamente sul sito Internet della BCE e sul sito Internet della Banca d'Italia dedicato al TIBER-IT[13].

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

Di seguito sono descritti i principali attori, ruoli, responsabilità e le interazioni tra le principali parti interessate (*stakeholders)* coinvolte nelle attività di gestione e implementazione del TIBER-IT. I principali ruoli e attori coinvolti in un test TIBER-IT sono:

- il Gruppo di coordinamento del TIBER-IT (TIBER-IT *Steering Committee*, TIBER-IT SC);
- il TIBER *Cyber Team* (TCT) e il *Team Test Manager* (TTM);
- il *White Team* (WT) ed il *White Team Lead* (WTL);
- il *Blue Team* (BT);
- il fornitore di servizi di analisi della mincaccia (*Targeted Threat Intelligence Provider* – TI Provider);
- il fornitore di servizi di *Red Teaming* (RT Provider).

I principali portatori di interesse di un test TIBER-IT sono ben informati sui rispettivi ruoli e responsabilità per garantire che:

- il test sia condotto in modo controllato adottando un approccio basato sul rischio;
- sia stabilito un chiaro protocollo sui flussi di informazione tra gli attori rivelanti durante tutto lo svolgimento del test;
- il citato protocollo definisca chiaramente le modalità di archiviazione e condivisione delle informazioni tra tutte le parti interessate.

Una descrizione più dettagliata dei ruoli e delle responsabilità dei diversi soggetti coinvolti nel processo di un test TIBER-IT è presente nella matrice di assegnazione delle responsabilità (RACI) riportata nell'allegato I: "Matrice RACI del TIBER-IT e principali risultati".

3.2.1 Gruppo di coordinamento del TIBER-IT (TIBER-IT *Steering Committee, SC*)

Per assicurare i compiti di coordinamento, aggiornamento e implementazione del TIBER-IT e la definizione del programma annuale e pluriennale di test, sarà istituito un comitato di alto livello tra le Autorità denominato Gruppo di coordinamento del TIBER-IT (TIBER-IT SC), composto da rappresentanti della Banca d'Italia, della Consob e dell'IVASS. Il TIBER-IT SC è presieduto da un rappresentante con adeguata *seniority* di una delle Autorità.

Il TIBER-IT SC supporta gli organi competenti delle Autorità nel rilascio di una comunicazione di avvenuto svolgimento del test attestante che il processo sia stato condotto in conformità al *framework* TIBER-EU e ai requisiti della presente Guida.

---

13 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.

Nel caso in cui l'entità non stia conducendo il test nello spirito del *framework* TIBER-EU e secondo i requisiti della presente Guida il TIBER-IT SC viene eventualmente consultato dal TTM circa la proposta di invalidare il test, in quanto non riconoscibile come test TIBER.

3.2.2 TIBER *Cyber Team* (TCT) e *Team Test Manager* (TTM)

Il TIBER *Cyber Team* (TCT) è composto da rappresentanti delle Autorità finanziarie che adottano la presente Guida ed è supportato da un gruppo stabile di risorse assicurate dalla Banca d'Italia[14].

Il TCT funge da punto di contatto[15] per le richieste di informazioni relative al TIBER-IT e ai test TIBER di tipo transfrontaliero; cura l'implementazione e propone eventuali aggiornamenti della Guida nazionale TIBER-IT per il sistema finanziario italiano, in collaborazione con altre autorità nazionali rilevanti ai fini della resilienza cyber. Il TCT inoltre supporta la pianificazione e coordinamento per l'esecuzione dei test TIBER-IT.

Il TCT facilita i test TIBER-IT in tutto il settore finanziario, fornisce supporto e conoscenze specialistiche ai WTLs. Il TCT facilita il dialogo tra tutte le parti interessate, comprese, se ritenuto opportuno, le funzioni di supervisione e sorveglianza.

Il TCT mantiene i contatti con altri TCTs in altre giurisdizioni e con i membri del TKC su base continuativa.

Per ogni test TIBER-IT è designato un *TIBER-IT Test Manager* (TTM) come principale punto di contatto per il WT; il TTM è responsabile per la verifica che l'entità effettui il test in modo uniforme e controllato, in conformità con la presente Guida. Il TTM è supportato nei suoi compiti e attività dal TCT. Data l'importanza del ruolo del TTM può anche essere nominato un suo sostituto, che lo affianca nelle attività.

Se nel corso di un test TIBER-IT l'entità non esegue l'esercizio nello spirito del *framework* TIBER-EU e in aderenza ai requisiti della presente Guida, il TTM può raccordarsi per l'invalidazione del test con il TIBER-IT SC e per le necessarie proposte agli organi decisionali della competente Autorità.

Il TTM svolge anche un ruolo chiave nel caso in cui ci siano significative deviazioni dalla pianificazione originale, discutendone con il WT.

Il TTM concorda il perimetro di applicazione (*scope*) e gli scenari e assicura che il test sia eseguito secondo il piano e che sia conforme al TIBER-IT e a tutti i requisiti pertinenti; ciò è importante per il mutuo riconoscimento da parte di altre giurisdizioni.

Per assicurare che tutti gli attori coinvolti in un test TIBER-IT adottino un approccio collaborativo, trasparente e flessibile, è necessaria una stretta

---

14 Servizio Supervisione mercati e sistemi di pagamento di Banca d'Italia, Divisione Continuità di servizio del sistema finanziario che non ha responsabilità dirette di supervisione o sorveglianza sulle entità finanziarie.

15 Il seguente indirizzo email tiber-it@bancaditalia.it è il punto di contatto unico per ogni richiesta relativa al TIBER-IT.

cooperazione tra il TTM e il WTL durante tutte le fasi del processo di test. In particolare, il TTM dovrebbe anche avere contatti diretti con il TI Provider e il RT Provider quando richiesto. Inoltre, laddove vi siano decisioni cruciali da prendere o laddove sorgano divergenze di opinione, sia il TTM che il WTL dovrebbero avere una linea formale di escalation interna verso i rispettivi vertici e/o organi decisionali. Per le entità finanziarie, ad esempio, tali linee formali sono rappresentate da: il responsabile della sicurezza delle informazioni (es. CISO), il direttore operativo (es. COO), il responsabile dei rischi (es. CRO) o qualsiasi altro alto funzionario con sufficiente autonomia decisionale.

Il TTM è indipendente dal WT e non è responsabile delle azioni del WT, dello svolgimento del test, dei risultati o del piano di rimedio (*Remediation Plan)*.

3.2.3 *White Team* (WT) e *White Team Lead* (WTL)

Per ogni test TIBER-IT, l'entità finanziaria stabilisce un *White Team* (WT), guidato da un apposito *White Team Lead* (WTL). Il WT è responsabile dell'individuazione del perimetro e dell'esecuzione del test, dell'acquisizione dei servizi, dei rapporti con tutte le altre parti, e rimane responsabile della gestione dei rischi durante il test.

Il WT è composto da personale con un'adeguata conoscenza delle funzioni critiche testate e da personale dell'entità finanziaria con una adeguata *seniority*, posizionato ai vertici della procedura di escalation relativa agli incidenti di sicurezza. I membri nel WT devono essere gli unici a conoscenza del test TIBER-IT all'interno dell'entità finanziaria, ne consegue che il WT deve essere mantenuto il più ristretto possibile per garantire che la conoscenza del test sia ridotta al minimo.

Il WT è responsabile della pianificazione e della gestione complessiva del test, in conformità con la presente Guida e con il *framework* TIBER-EU.

Il WTL coordina tutte le attività del test, incluse quelle relative all'acquisizione e gestione dei servizi erogati dai TI e RT Providers a i possobili incontri con le Autorità.

Maggiori dettagli sui ruoli, le responsabilità e la composizione ideale del WT possono essere trovati nel documento TIBER-EU *White Team Guidance*[16].

3.2.4 *Blue Team* (BT)

Per ogni test TIBER-IT, il *Blue Team* (BT) è composto da tutto il personale (non membro nel WT) dell'entità finanziaria sottoposta a test, comprese le terze parti, specialmente coloro che gestiscono i sistemi (e le relative persone, processi e tecnologie) dell'entità sottoposta a test. In particolare, il BT include anche il personale responsabile della difesa dei sistemi informativi dell'entità assicurando un adeguato livello di sicurezza nei confronti di attori di minacce informatiche. È fondamentale che il BT non sia a conoscenza del test

16 https://www.ecb.europa.eu/pub/pdf/other/ecb.tibereu.en.pdf

durante il suo svolgimento e sia completamente escluso dalla preparazione e dall'esecuzione del test TIBER-IT.

Solo durante la fase di chiusura (*closure*) il BT sarà informato del test e i suoi principali rappresentanti partecipano alle attività di *replay* e *follow-up*. Durante la fase di chiusura il BT è responsabile della stesura del BT Report (*Blue Team report*), una relazione tecnica che riguarda, per ogni scenario di minaccia testato, le azioni di difesa eseguite dal BT durante le attività del RT.

3.2.5 Fornitore di *Threat intelligence* (TI Provider)

Il TI Provider è un fornitore esterno i cui servizi sono stati acquisiti dal WT secondo gli standard e i requisiti minimi stabiliti nel documento TIBER-EU *Services Procurement Guidelines*. Il TI Provider raccoglie informazioni mirate sull'entità, emulando la ricerca che sarebbe eseguita da un *hacker* esperto e fornisce queste informazioni all'entità sotto forma di un TTI Report. Il TI Provider dovrebbe utilizzare molteplici fonti di *intelligence* per fornire una valutazione quanto più accurata e aggiornata possibile.

Il TI Provider lavora in stretta collaborazione con il RT Provider, contribuendo a sviluppare gli scenari di attacco per il *red team* test, nonché eventuali nuovi requisiti derivanti dall'analisi di intelligence che si manifestano durante l'esecuzione del *red team* test. Il TI Provider dovrebbe dare un contributo alla relazione finale rilasciata all'entità.

3.2.6 Fornitore di *Red Teaming* (RT Provider)

Il RT Provider è un fornitore esterno, i cui servizi sono stati acquisiti dal WT secondo gli standard e i requisiti minimi stabiliti nel documento TIBER-EU *Services Procurement Guidelines*. Il suo obiettivo è quello di tentare di violare i presìdi di sicurezza dell'entità, seguendo una metodologia di *red teaming* rigorosa ed etica, 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 dal RT Provider e dall'entità finanziaria.

Il RT Provider elabora il *Red Team Test Plan* ed esegue il test TIBER-IT dei sistemi e dei servizi *target*, concordati nella fase di *scoping* (vedere anche § 3.5). Dopo il completamento della fase di *testing*, il RT Provider effettua una analisi del test e delle problematiche rilevate e redige un *Red Team Test Report*.

Il RT Provider lavora a stretto contatto con il TI Provider durante tutte le fasi del test al fine di aggiornare le informazioni derivanti dalla *threat intelligence* e gli scenari di attacco previsti con quanto di più pertinente e recente. Infine, il RT Provider è opportuno che a collabori con il TI Provider anche al fine di sviluppare e consegnare all'entità il *Red Team Test Report*.

3.3 Gestione dei rischi durante l'esecuzione dei test TIBER-IT

I test TIBER-IT sono condotti sui sistemi che sostengono le funzioni critiche di un'entità in ambiente di produzione, tenendo conto della superficie di attacco reale e delle effettive debolezze dell'entità. Pertanto, l'esecuzione del test

comporta potenziali rischi. Di conseguenza, devono essere applicati adeguati controlli per garantire che l'esecuzione del test non infici la corretta operatività[17] dell'entità finanziaria e dei suoi clienti.

Nell'ambito della gestione del rischio del test, il WT può interrompere il test in qualsiasi momento, se ritiene che la sua continuazione comporti un rischio inaccettabile per l'entità. Il WT assicura un'appropriata gestione del rischio e che adeguati controlli siano comunicati e compresi da tutte le parti interessate, tenendo conto del quadro di controlli interni e della governance dell'entità finanziaria.

Le funzioni e i sistemi informativi oggetto dei test TIBER-IT contengono informazioni protette ai sensi di diverse previsioni 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 e l'integrità, la disponibilità e la riservatezza delle suddette informazioni attraverso il ricorso ad adeguati strumenti di gestione del rischio.

Alla luce di quanto precede, l'entità deve effettuare una analisi del rischio prima del test per garantire che adeguati processi, procedure e controlli siano adottati in linea con l'esistente quadro di gestione del rischio dell'entità. Il WT elaborerà un piano di gestione del rischio per il test, secondo le pratiche in essere presso l'entità, al fine di identificare, analizzare e mitigare i rischi. Il piano di gestione del rischio, che deve essere aggiornato ad ogni modifica significativa, comprenderà almeno:

- l'indicazione di quali tattiche, tecniche e procedure (TTPs) non possono essere utilizzate;
- l'indicazione di quali funzioni, sistemi e altri potenziali obiettivi sono al di fuori del perimetro di test;
- l'indicazione di quali misure di emergenza sono state previste e come il WT reagirebbe in caso di potenziali interruzioni causate dal test.

Il WT ha la responsabilità di garantire che il RT Provider prepari il suo piano di test entro i limiti di questa analisi del rischio.

Il WT, i TI e RT Providers concordano un nome in codice da utilizzare in tutta la documentazione durante il test, al fine di proteggere l'identità dell'entità finanziaria e la natura del test.

Al fine di assicurare la riservatezza del test, il WT deve limitare la conoscenza dello stesso e delle relative informazioni a un ristretto gruppo fidato all'interno dell'entità, i cui membri hanno appropriati livelli di autonomia per prendere decisioni relative al test, secondo un approccio basato sul rischio.

I TI e RT Providers devono concordare con il WT le procedure per la gestione e la protezione delle informazioni durante il test e per la loro cancellazione a test concluso (vedere anche § 3.4.23.4.2).

---

17 In conformità con prassi ampiamente adottate relative ai TLPT e con i G7FE-TLPT, nello svolgimento dei test TIBER-IT, le entità finanziarie, in consultazione con le loro parti interessate, applicano controlli efficaci per ridurre il rischio di qualsiasi potenziale impatto sui dati dell'entità, di danni agli asset dell'entità e di interruzione ai servizi critici e/o alle operazioni essenziali presso l'entità o nel settore finanziario.

Per gestire efficacemente i rischi durante il test, il WT deve mantenere il controllo del processo per garantire che il test proceda in conformità con il perimetro, lo scenario, la pianificazione e il processo concordati.

3.4 Fase di preparazione (*preparation*)

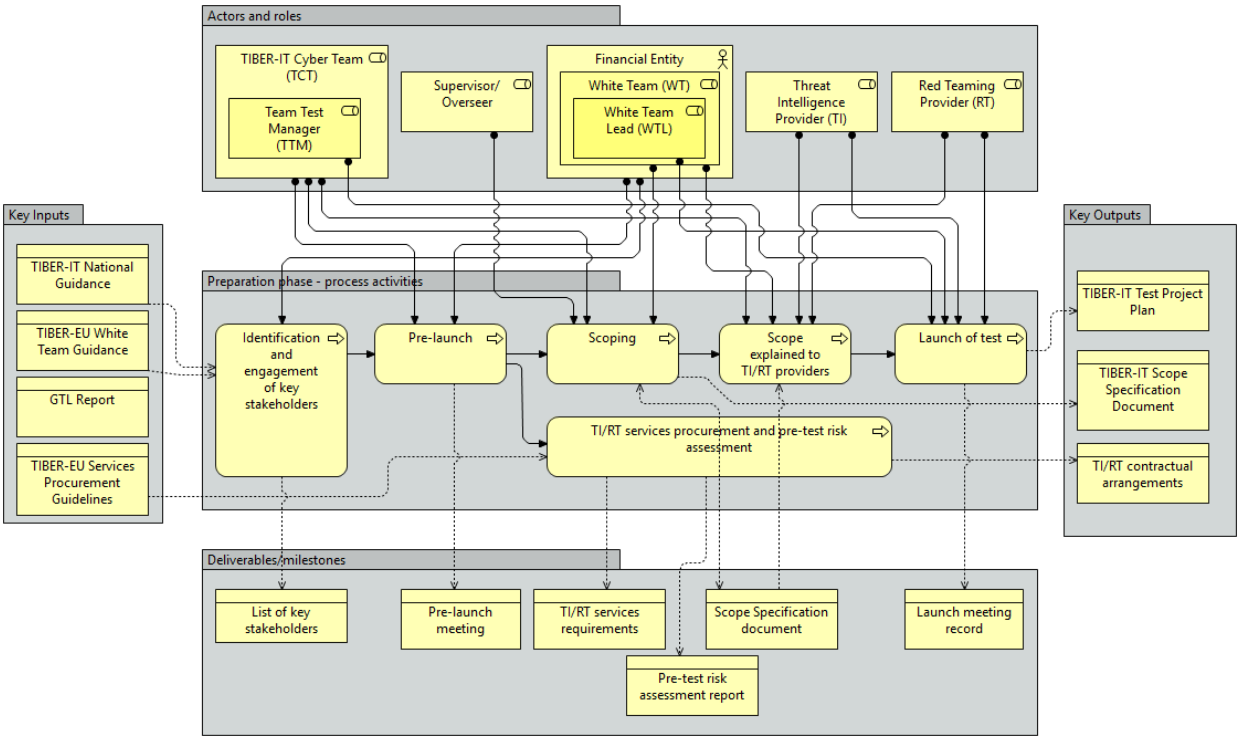
Ai fini dell'avvio della fase di preparazione (*preparation*), l'entità che intende sottoporsi al test comunica formalmente al TCT la disponibilità ad effettuare un test TIBER-IT.

Il TTM individuato per facilitare il test inizia a collaborare con l'entità partecipante. Viene stabilito il perimetro di applicazione del test e l'entità acquisisce i servizi di TI e RT. Questa fase di preparazione dura da quattro a sei settimane circa, esclusa la durata della procedura di acquisizione dei citati servizi.

All'inizio della fase di preparazione, il TCT richiede la costituzione di un WT e la nomina del WTL da parte dell'entità. Il WT è composto da un piccolo numero di personale esperto e/o nella posizione di prendere decisioni basate sul rischio per tutta la durata del test. Una volta costituito il WT, l'entità informa il TCT della sua composizione. Il WTL assicura che il WT sia a conoscenza del test TIBER-IT, dei requisiti di segretezza e del processo che il team dovrebbe seguire in caso avvengano determinati eventi (ad es. nel caso in cui il BT rilevi l'attacco simulato e attui la procedura di escalation interna relativa ad incidente di sicurezza).

La fase di preparazione inizia con il *pre-launch meeting*, che è seguito dall'acquisizione dei servizi, dallo *scoping* e porta al *launch meeting* (Figura 3).

Figura 3: PANORAMICA DEL PROCESSO TIBER-IT – FASE DI PREPARAZIONE



3.4.1 *Pre-launch meeting*

Il WTL tiene il *pre-launch meeting* con il TTM e i membri del WT che il WTL desidera invitare. Ulteriori linee guida per il WT sono dettagliate nella TIBER-EU *White Team Guidance* e nelle citate TIBER-EU Services Procurement Guidelines, che possono essere discusse durante la riunione.

Durante il *pre-launch meeting*, il TTM informa l'entità sui requisiti per:

- il processo di test nel *framework* TIBER-EU e la sua ulteriore contestualizzazione come previsto nella presente Guida;
- i ruoli e le responsabilità delle parti interessate;
- i protocolli di sicurezza (compreso il trasferimento sicuro dei documenti);
- le condizioni contrattuali (compresa la condivisione della documentazione da parte dei TI e RT Providers);
- la pianificazione del test.

Per facilitare la condivisione di informazioni in maniera libera, affidabile e sicura, le parti coinvolte – compresi i membri del WT e i TI e RT Providers – dovrebbero siglare un accordo di riservatezza (NDA).

In questa fase è stabilita una data per l'avvio del test.

3.4.2 Acquisizione dei servizi (*procurement*)

Dopo, o anche eventualmente in parallelo con il *pre-launch meeting*, il WT inizia il processo di acquisizione dei servizi (*procurement)*. Il TCT esercita un certo grado di giudizio sull'opportunità di consentire al WT di avviare il citato processo in parallelo con il *pre-launch* o se consentirlo solo una volta che il *pre-launch* e lo *scoping* siano stati completati.

Data la natura sensibile dei test TIBER-IT, il WT sottopone i TI e RT Providers ad un rigoroso processo di *due diligence* basato su criteri di selezione volti a verificare che il fornitore esterno sia in grado di utilizzare professionisti altamente qualificati e specializzati nello svolgimento di attività avanzate di *ethical hacking*. Alcuni di questi criteri includono referenze professionali nei settori della *threat intelligence* e dell'*ethical hacking*, il livello di competenza del personale da far partecipare al test, il rispetto di un codice di condotta e un adeguato livello di garanzia.

In particolare, poiché il WT è responsabile dell'acquisizione dei servizi di TI e RT, la procedura deve seguire le indicazioni e i requisiti minimi dettagliati nelle citate TIBER-EU *Services Procurement Guidelines*.

In dettaglio, poiché i test sono condotti su sistemi in ambiente di produzione, il WT deve procurarsi TI e RT Providers competenti, qualificati, abili e con l'esperienza necessaria per condurre tali test, al fine di evitare rischi dovuti a fornitori di servizi inesperti o non qualificati.

Un test TIBER-IT deve essere condotto da fornitori di terze parti indipendenti, escludendo la possibilità di utilizzare risorse interne. Ove possibile, le entità assicurano che i fornitori appaltati siano accreditati e certificati da organismi

riconosciuti in materia secondo gli standard di settore. Il TTM fornirà il supporto necessario relativamente al *procurement*.

Durante il *procurement*, il WT svolge le seguenti attività:

- garantire il rispetto di quanto previsto dal TIBER-EU *Services Procurement* Guidelines e delle migliori pratiche per individuare potenziali fornitori di TI/RT in grado di soddisfare gli obiettivi del test;
- indire una manifestazione di interesse (es. una *request for proposal* – RFP) in conformità con la presente Guida e della pertinente legislazione in materia di acquisizione di servizi;
- valutare le offerte, quindi intervistare e selezionare i fornitori appropriati e,
- stabilire condizioni per la condivisione, la riservatezza e la conservazione dei diritti di proprietà intellettuale.

Il WT assicura che vi sia un accordo con i TI e RT Providers almeno sui seguenti aspetti: perimetro di applicazione del test; limiti; tempistica e disponibilità dei fornitori; contratti; azioni da intraprendere e responsabilità (compresa l'assicurazione ove applicabile).

I contratti tra WT e i TI e RT Providers includono tra l'altro:

- requisiti di sicurezza e riservatezza che siano almeno altrettanto rigorosi di quelli rispettati dall'entità testata;
- previsioni di adeguate misure di tutela[18];
- clausole relative alla non divulgazione e alla riservatezza, al trattamento dei dati, alla protezione e alla distruzione dei dati e alle disposizioni sulla notifica delle violazioni;
- le attività non consentite durante il test, quali la distruzione di apparecchiature, la modifica incontrollata di dati o programmi, la compromissione della continuità dei servizi critici, il ricatto, la minaccia o corruzione dei dipendenti e la divulgazione dei risultati dei test.

Una volta che l'acquisizione dei servizi è stata completata, il WT attesta, al meglio delle sue conoscenze, che il processo di approvvigionamento ha aderito sia alla TIBER-EU *White Team Guidance* sia alle TIBER-EU *Services Procurement Guidelines*.

3.4.3 Perimetro di applicazione del test (*scoping*)

L'obiettivo principale dell'attività di *scoping* è che il WT e il TTM concordino sul perimetro di applicazione del test TIBER-IT e sull'identificazione delle funzioni critiche che devono essere incluse. L'entità può decidere, a sua discrezione, di includere ulteriori funzioni non critiche (ad es. persone, processi e tecnologie) nel perimetro di applicazione del test, a condizione che queste non influiscano negativamente sul test delle predette funzioni critiche. Di solito, il perimetro del test TIBER-IT comprenderà anche i sistemi,

[18] Es. coperture assicurative relative alle attività dei TI e RT Providers non precedentemente concordate nel contratto e/o che derivino da dolo, negligenza, ecc. (vedasi anche TIBER EU Services Procurement Guidelines).

le persone e i processi di business alla base delle FC dell'entità che sono esternalizzati a terze parti.

Ai fini di un test TIBER-IT, le attività di testing rilevanti devono essere eseguite sui sistemi in ambiente di produzione dell'entità. Tuttavia, l'entità può anche includere nel perimetro del test sistemi di pre-produzione, testing, backup e ripristino.

Ai fini dello *scoping*, sia il TTM che il WT dovrebbero avere una conoscenza approfondita del modello di business, delle funzioni e dei servizi dell'entità da sottoporre a test.

In linea con le pratiche di gestione del rischio operativo in essere presse l'entità, il WT dovrebbe condurre (o basarsi su) una *Business Impact Analysis* (BIA) per definire le FC. Durante l'identificazione delle FC e dello *scope* del test, il WT può anche fare riferimento al GTL report per fornire un contesto aggiuntivo e le minacce da affrontare, e per mappare i possibili scenari di minaccia alle FC. Il TTM, con l'aiuto del TCT, si consulterà con le Autorità di supervisione o sorveglianza competenti per assicurarsi che le appropriate FC siano prese in considerazione nell'ambito dello *scoping*.

Il WT, prima dello *Scoping meeting*, deve compilare e distribuire a tutte le parti coinvolte una bozza del documento relativo al perimetro del test *(draft Scope Specification document)*[19]. Questo documento identifica lo *scope* del test TIBER-IT e include dettagli su quali sistemi chiave e servizi sono alla base di ogni FC. Sulla base di queste informazioni, il WT imposta gli obiettivi (*flags*)[20] che il RT Provider deve raggiungere durante il test; le *flags* devono essere discusse e approvate dal TTM. Tali *flags* possono tuttavia essere modificate su base iterativa durante il test, in seguito alla raccolta di TI e all'evoluzione del test; in questi casi anche il piano di valutazione del rischio (§ 3.3) dovrebbe essere aggiornato.

Lo *Scope Specification document* finale è concordato con il TTM nel corso di uno *Scoping meeting* organizzato dal WT per tutte le parti interessate (es. WT, TTM ed eventualmente i TI e RT Providers).

È fondamentale che il perimetro di applicazione del test TIBER-IT sia firmato al livello di Consiglio di Amministrazione dell'entità.

Se la fase di *procurement* è stata conclusa, il processo di *scoping* e lo *scoping meeting* possono includere i TI e RT Providers. In caso contrario, è consigliato che il WT e il TTM ne discutano prima dello *scoping meeting* e che sia organizzato un successivo incontro con i TI e RT Providers per spiegare le FC e i sistemi che le supportano.

---

19 Basato sul TIBER-EU ***Scope Specification template***: https://www.ecb.europa.eu/paym/cyber-resilience/tiber-eu/shared/pdf/Final_TIBER-EU_Scoping_specification_template_July_2020.pdf

20 Le ***flags*** sono sostanzialmente gli obiettivi che il RT Provider deve tentare di raggiungere durante il test, utilizzando una varietà di tecniche.

3.4.4 Avvio del test

L'incontro di avvio del test (*launch meeting*) è una riunione che coinvolge tutte le parti interessate (compresi il TTM, il WT e i TI e RT Providers), la cui agenda comprende il processo di *testing*, le aspettative, così come il *draft project plan* TIBER-IT. Lo scopo del *launch meeting* è quello di comunicare le responsabilità, la pianificazione e l'esecuzione del test TIBER-IT.

Una volta che il *procurement* è stato completato e i principali accordi contrattuali sono in essere, il WT deve preparare un *draft project plan*. Il *draft project plan* deve includere un programma di incontri tra il WT, i TI e RT Providers e il TTM. Il *project plan* deve essere distribuito a tutte le parti interessate dal WTL prima del *launch meeting* e copre:

- l'organizzazione dei test e la logistica;
- gli obiettivi del test in relazione al GTL Report;
- le funzioni testate e le relative persone, processi e tecnologie;
- il calendario dei preparativi e dei test;
- gli obiettivi specifici;
- i confini;
- la gestione del rischio;
- la comunicazione durante le prove;
- altre informazioni pratiche relative al test.

Un nome in codice per l'entità deve essere scelto e utilizzato da tutte le parti interessate quando si riferiscono all'entità durante tutte le fasi del processo di test per assicurare la riservatezza e la segretezza del test.

3.5 Fase di test (*testing*)

La fase di test (*testing*) inizia una volta che il perimetro di applicazione sia stato concordato, i TI e RT Providers siano stati selezionati e tutte le parti interessate siano state informate circa i loro ruoli e responsabilità.

Il *testing* prevede la raccolta di informazioni di TI relative all'entità testata, grazie alle quali vengono sviluppati scenari di minaccia dettagliati dal TI Provider. Il RT Provider si baserà su questi e svilupperà scenari di attacco per creare il TIBER-IT *Red Team Test Plan*[21] prima dell'esecuzione del test.

Gli scenari che simulano attacchi cyber realistici devono essere basati sui risultati del *TTI Report* e sulle indicazioni del *GTL Report*. Mentre il GTL *Report* identifica le minacce principali relative al settore finanziario, esso può essere utilizzato come prezioso contributo per sviluppare il TTI *Report*, il quale fornisce una visione dettagliata sulla superficie di attacco dell'entità e sui suoi presìdi di difesa in essere. Inoltre, il TTI *Report* supporta lo sviluppo di scenari di attacco attuabili e realistici, attraverso l'emulazione delle TTPs dei reali attori della minaccia e portando alla realizzazione di una simulazione realistica.

---

21 https://www.ecb.europa.eu/paym/cyber-resilience/tiber-eu/shared/pdf/Final_TIBER-EU_Guidance_for_the_Red_Team_Test_Plan_July_2020.pdf

Il GTL *Report* per il settore finanziario italiano è fornito dal TCT[22], mentre il TTI *Report* è preparato dal TI Provider. Il GTL *Report* può essere aggiornato dal TCT su base continuativa, generalmente almeno una volta l'anno, in modo da prendere tempestivamente in considerazione nuovi attori di minaccia, TTP e vulnerabilità.

La fase di test prosegue con il passaggio di consegne tra i TI e RT Providers; a questa attività fa seguito lo sviluppo del *Red Team Test Plan* e degli scenari di attacco e conduce all'esecuzione del test.

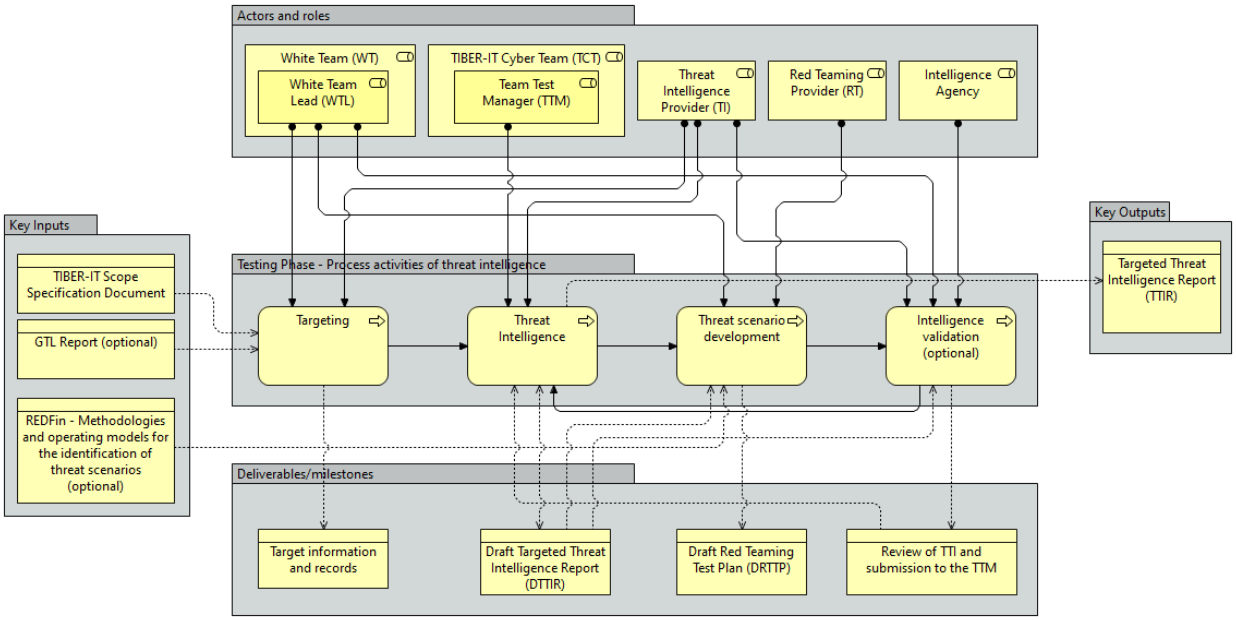
3.5.1 *Targeted Threat Intelligence* (TTI) e identificazione degli scenari della minaccia

Qualora sia disponibile il GTL *Report*, il TI Provider ne sfrutta le informazioni per sviluppare scenari di minaccia specifici per l'entità sottoposta a test da includere nel TTI *Report*. Nel farlo, il TI Provider dovrebbe consultare il RT Provider per garantire che gli scenari sviluppati siano perseguibili (Figura 4).

Durante il processo TTI, il TI Provider raccoglie, analizza e diffonde informazioni di intelligence focalizzate sulle FC relative a due principali aree di interesse:

- identificazione del bersaglio (*targeting*): intelligence o informazioni su potenziali superfici di attacco dell'entità;
- identificazione delle minacce (*threat intelligence*): intelligence o informazioni sugli attori della minaccia rilevanti e probabili scenari di minaccia.

Figura 4: PANORAMICA DEL PROCESSO TIBER-IT – FASE DI TEST – PROCESSO DI TTI



22 Sotto il coordinamento del TCT e sulla base di disposizioni specifiche, il GTL Report può essere sviluppato in stretta collaborazione con altre parti interessate. In particolare, il TCT potrebbe avvalersi del sostegno fornito da altre autorità finanziarie, dalle funzioni di ***cyber security*** e ***risk governance*** aziendali, dal CERTFin e da altre agenzie di intelligence e sicurezza.

In combinazione con gli input opzionali forniti dal WT, il TI Provider utilizza le informazioni acquisite tramite le attività di *targeting* e *threat intelligence* per sviluppare gli scenari della minaccia.

L'attività di *targeting* viene eseguita dal TI Provider, dal punto di vista dell'attaccante, per ottenere un quadro preliminare dettagliato dell'entità e dei suoi punti deboli. Il risultato di questa attività è l'identificazione, sulla base delle FC e per ogni sistema, delle superfici di attacco in termine di persone, processi e tecnologie relativi all'entità e della sua impronta digitale globale (*digital footprint*). Ciò può includere informazioni che vengono pubblicate intenzionalmente dall'entità e altre informazioni interne che sono state divulgate involontariamente, come i dati dei clienti, materiale confidenziale o altre informazioni che potrebbero essere una risorsa utile per un attaccante.

Le attività di *targeting* sono un prezioso input e un elemento centrale del TTI *Report* e hanno l'obiettivo di personalizzare il profilo della minaccia e gli scenari. Poiché il *targeting* rende note alcune delle superfici di attacco dell'entità e identifica gli obiettivi iniziali, è anche un prezioso input per le successive attività di *targeting* più profonde e focalizzate del RT Provider.

Per quanto riguarda le attività di *threat intelligence*, il TI Provider raccoglie, analizza e diffonde informazioni di intelligence sugli attori della minaccia rilevanti e sui probabili scenari della minaccia, con l'obiettivo di presentare un quadro plausibile del panorama delle minacce cyber, basato su un'analisi delle minacce fondata su dati comprovati e specificamente adattata all'ambiente aziendale e al business dell'entità, compresi i fornitori di terze parti critici. Il TI Provider può utilizzare il GTL *Report* per integrare ulteriormente l'identificazione delle minacce.

L'output risultante dal processo di identificazione delle minacce è una sintesi delle principali minacce, con profili dettagliati delle minacce più pertinenti e potenziali scenari in cui un rilevante attore della minaccia potrebbe prendere di mira l'entità.

Al fine di rendere la raccolta di informazioni quanto più efficiente possibile e di garantire che essa sia rilevante per il perimetro di applicazione del test e per l'attività dell'entità, il WT dovrebbe fornire al TI Provider informazioni complete per la *targeted threat intelligence*, che includono:

- una panoramica di business e tecnica di ciascun sistema che supporta le FC incluse nel perimetro del test;
- l'attuale analisi delle minacce e/o il registro delle minacce;
- eventuali esempi di attacchi recenti.

L'intero processo TTI dura circa cinque settimane.

Il prodotto del processo TTI è il TTI *Report*, che è un report di *threat intelligence* su misura per l'entità sottoposta al test. Il suo scopo è quello di coadiuvare lo sviluppo degli scenari di attacco, utilizzando una specifica analisi della minaccia e attività di ricognizione (*reconnaissance*) focalizzata all'entità testata, prendendo in considerazione attori reali individuati all'interno del

panorama delle minacce. Il TI Provider è responsabile dello sviluppo e della produzione del TTI *Report*[23] e lo mette a disposizione del RT Provider, che utilizza il contenuto del TTI *Report* per sviluppare gli scenari di attacco in un *Red Team Test Plan*. Il TTI *Report* costituisce una solida base probatoria per il test di *red teaming* proposto. A tal proposito, tre output sono particolarmente rilevanti:

- scenari su misura, che supporteranno la definizione di un *Red Team Test Plan* realistico ed efficace;
- obiettivi e motivazioni dell'attore della minaccia, che aiuteranno il RT Provider nel suo tentativo di catturare le *flags* concordate nella fase di *scoping*;
- evidenze convalidate che sosterranno il *business case* successivo al test relativo al miglioramento e alle azioni di rimedio.

Al fine di creare scenari di minaccia realistici e che descrivano attacchi contro l'entità, tali scenari devono essere basati sulle evidenze disponibili dei reali attori della minaccia, insieme ad altri dati di intelligence relativi all'entità. L'adozione di diverse pratiche di raccolta di informazioni (*information gathering*) e analisi di intelligence è caldamente incoraggiata. Si raccomanda inoltre un approccio strutturato basato su metodologie e modelli operativi standardizzati per l'individuazione degli scenari della minaccia[24].

Il TI Provider deve sempre dimostrare un comportamento profondamente etico e le attività di TTI devono sempre essere condotte nel rispetto delle leggi applicabili.

Nel mondo reale gli attori malevoli potrebbero non avere vincoli di tempo o risorse come quelli a cui sono sottoposti i TI e RT Providers, avendo la possibilità di trascorrere mesi a preparare un attacco e non essendo limitati da limiti morali, etici e legali. Allo stesso modo, i sistemi alla base delle FC in genere non hanno una ampia esposizione sulla rete pubblica. Sia che si tratti di sistemi interni sviluppati ad hoc oppure di sistemi esterni che si estendono su più organizzazioni con infrastrutture di collegamento comuni, la conoscenza del funzionamento di questi sistemi da parte dei TI e RT Providers può essere limitata rispetto a quella in possesso di reali *cyber-attackers* che abbiano la capacità e il tempo di studiarli ampiamente.

Pertanto, l'entità determina la quantità di informazioni che è disposta a divulgare ai TI e RT Providers, per garantire che essi abbiano il livello adeguato di conoscenza per simulare attacchi avanzati. In questo modo, il TIBER-IT rifletterebbe un tipo di test "*grey box*" in contrasto con l'approccio di tipo "*black box*".

---

23 https://www.ecb.europa.eu/paym/cyber-resilience/tiber-eu/shared/pdf/Final_TIBER-EU_Guidance_for_Target_Threat_Intelligence_July_2020.pdf

24 Per facilitare l'identificazione di scenari di minaccia realistici, le entità finanziarie possono fare riferimento e sfruttare il documento del progetto REDFin di ABI Lab "***Methodologies and operating models for the identification of threat scenarios***".

L'esperienza dimostra che più informazioni rilevanti un'entità fornisce ai TI e RT Providers, più l'entità sottoposta al test trarrà vantaggio dallo stesso. Se l'entità dispone di capacità o di una funzione interna di TI e la riservatezza del test può essere mantenuta, il TI Provider può coordinarsi con essa per raccogliere informazioni pertinenti a sostegno dello sviluppo del TTI *Report*.

Una volta che il *draft* TTI *Report* è stato completato, il TI Provider lo condivide con il WT, il TTM e il RT Provider, per intraprenderne congiuntamente una revisione approfondita al fine di correggere eventuali errori fattuali e discutere eventuali problemi che potrebbero sorgere. Sulla base del *draft* TTI *Report*, il WT e il TTM possono decidere di aggiornare o modificare le *flags* stabilite durante la fase di *scoping*. Il TTI *Report* dovrebbe essere condiviso con i citati attori con largo anticipo prima della riunione di trasferimento (*handover meeting*) tra i TI e RT Providers. Inoltre, ove necessario, le agenzie di sicurezza e di intelligence nazionali ritenute pertinenti per ciascun test potrebbero essere contattate dal TTM per fornire un feedback sul *draft* TTI *Report*.

Lo sviluppo degli scenari di attacco è il punto di transizione chiave tra i TI e RT Providers. Tale attività viene svolta poco prima o in parallelo con la citata eventuale valutazione del *draft* TTI *Report* da parte delle agenzie di sicurezza o di intelligence nazionale.

Il RT Provider sviluppa e integra gli scenari di attacco in una *draft Red Team Test Plan*, utilizzando gli scenari inclusi nel *draft* TTI *Report* e in accordo al documento TIBER-IT *Test Scope Specification*. In questa fase, può essere tenuto un *workshop*, tra il WT, il TTM e i TI e RT Providers, per riesaminare gli scenari presentati dal TI Provider e per consentire al RT Provider di sviluppare il *Red Team Test Plan*.

Le attività del *workshop* includono:

- una panoramica del TTI *Report* e dei possibili cambiamenti a seguito di eventuali commenti da parte delle agenzie di intelligence e di sicurezza nazionali;
- eventuali commenti sul TTI *Report* da parte del TTM;
- una presentazione del *draft Red Team Test Plan*, compresa la mappatura delle FC agli scenari, le *flags*, i possibili aiuti previsti (*legs-up*)[25], la mitigazione dei rischi, le procedure di escalation, le date di inizio e fine dei test e una previsione della data di consegna del *draft Red Team Test Report* da parte del RT Provider.

Dopo il *workshop*, il TI Provider, ove necessario, aggiorna e produce una versione finale del TTI *Report* da consegnare all'entità. Analogamente, anche il RT Provider, ove necessario, aggiorna il *draft Red Team Test Plan* alla luce dei risultati del workshop e dei rischi identificati.

---

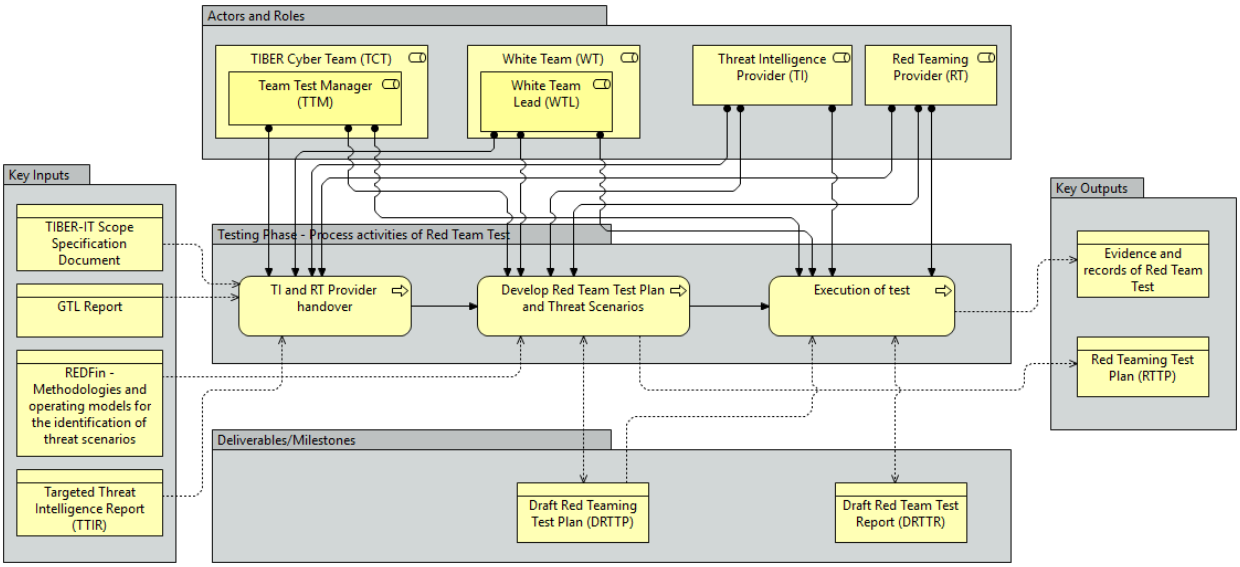
25 Se durante il processo di test il RT Provider non fosse in grado di passare alla fase successiva a causa di vincoli di tempo o perché il BT fosse riuscito a proteggersi, il RT Provider, con l'accordo del WT e del TTM, può ricevere un "vantaggio": il WT essenzialmente concede al RT Provider l'accesso al sistema, alla rete interna, ecc. per continuare il test e concentrarsi sulla prossima ***flag*** da catturare.

In qualsiasi circostanza è vietato ai TI e RT Providers di utilizzare qualunque di queste informazioni sui rischi e sulle minacce in qualsiasi altro contesto al di fuori del test, sia singolarmente sia in maniera aggregata. Il TTI *Report* è altamente confidenziale ed è necessario proteggere i suoi contenuti dall'essere divulgati o fatti trapelare al di fuori di questo ristretto gruppo di attori, anche all'interno del BT dell'entità.

3.5.2 Pianificazione del test di *Red teaming*

Una volta completato il processo di TTI, il RT Provider pianifica ed esegue il test TIBER-IT sui sistemi e servizi identificati che sono alla base di ogni FC nel perimetro di applicazione del test (Figura 5).

Figura 5: PANORAMICA DEL PROCESSO TIBER-IT – FASE DI TEST – PROCESSO DI RT



Questa fase deve consentire al RT Provider il tempo sufficiente per condurre un test realistico e completo, in cui vengono eseguite tutte le fasi di attacco e vengono raggiunti tutti gli obiettivi del test e le *flags* – concordati durante la fase di *scoping* e aggiornati durante il processo di TTI. Il tempo assegnato al test dovrebbe essere proporzionato al perimetro di applicazione, alle risorse dell'entità e alla disponibilità delle informazioni di supporto fornite dal WT. In generale, 10-12 settimane è una durata appropriata per il testing.

Prima dell'inizio del test, si tiene una sessione di *handover* tra TI e RT Providers, per fornire una spiegazione dettagliata del TTI *Report* e per discutere possibili scenari di minaccia per il test. A seguito della riunione di *handover*, il RT Provider integra ulteriormente gli scenari di attacco e finalizza il *Red Team Test Plan*, basandosi sul documento TIBER-IT *Scope Specification*, sul GTL *Report* e sul TTI *Report*.

Il RT Provider dovrebbe porre in essere un'ampia gamma di TTPs durante il test, utilizzando metodologie di test quali ricognizione, *weaponisation*, *delivery*, sfruttamento, controllo e movimento e azioni sull'obiettivo[26].

Nel preparare gli scenari di attacco e il *Red Team Test Plan*, il RT Provider provvede a:

- allineare i suoi obiettivi del test con quelli di ciascun attore;
- mappare gli obiettivi ai sistemi che supportano le FC;
- produrre scenari di attacco reali credibili per il test;
- progettare gli scenari di attacco in modo da fornire un quadro delle tecniche impiegate da ciascuna minaccia per condurre un attacco di successo;
- adattare la sua metodologia di attacco per simulare gli scenari di attacco reali;
- attingere al TTI Report, che rivela alcune delle superfici di attacco dell'entità, come base per attività di *targeting* più profonde e mirate;
- aggiungere alcuni elementi che testino le capacità di rilevamento e risposta del BT;
- indicare, in coordinamento con il WT, dove potrebbe essere necessario un aiuto (*legs-up*), qualora l'attacco non avesse successo;
- includere un adeguato piano per la gestione dei rischi che il test di *red teaming* pone ai sistemi nel perimetro di applicazione alle relative informazioni di business trattate;
- evitare qualsiasi azione che possa avere effetti destabilizzanti sulla stabilità finanziaria o sulla resilienza operativa del sistema finanziario italiano.

L'output della pianificazione del test è il *Red Team Test Plan* finale, che include gli scenari di attacco da eseguire e i controlli sui rischi che verranno applicati per assicurare che il test sia condotto in modo controllato.

Lo sviluppo dello scenario di attacco è un processo creativo. Gli scenari di attacco sono scritti dal punto di vista dell'attaccante e definiscono le *flags* da catturare. Nella scrittura dello scenario di attacco, il RT Provider dovrebbe indicare opzioni alternative per ciascuna delle fasi di attacco, basate su diverse TTPs utilizzate da attaccanti avanzati al fine di anticipare cambiamenti del contesto o nel caso in cui la prima opzione non funzioni. Le TTPs non possono semplicemente imitare gli scenari visti in passato, ma possono combinare le tecniche di vari attori rilevanti della minaccia, tra cui TTPs innovative che non sono ancora state utilizzate nella realtà, ma sono attese per il futuro. In questo caso si parla di "Scenario X", che consente una prospettiva futura su possibili attacchi. L'obiettivo dello Scenario X, che non è obbligatorio includere nel *Red Team Test Plan*, è quello di ipotizzare quali attacchi avanzati possano essere attesi nel prossimo futuro. Lo scenario può concentrarsi su una particolare TTP innovativa, non ancora utilizzata, eventualmente

[26] Si prega di fare riferimento al quadro TIBER-EU per ulteriori dettagli.

combinata con sviluppi della società che potranno avere un impatto sull'entità. L'attenzione dello Scenario X, tuttavia, rimane sulle funzioni critiche.

Considerando il disallineamento tra gli attaccanti cyber reali ed il RT Provider in termini di vincoli di tempo e risorse, compresi i confini morali, etici e legali, per facilitare un test più efficace ed efficiente, il WT può fornire ulteriori informazioni al RT Provider sugli scenari, comprese le relative persone, processi e sistemi. Sulla base di queste informazioni il RT Provider può sviluppare ulteriori intuizioni e fare un uso migliore del tempo. In ogni caso, l'esperienza mostra che esiste una correlazione diretta tra la pertinenza delle informazioni aggiuntive che il WT fornisce al fornitore e il benefit complessivo che l'entità trarrà dal test di *red teaming*.

Inoltre, durante la fase di test, il ruolo del TI Provider può essere potenziato, fornendo al RT Provider una *threat intelligence* continua, che può risultare in una ricognizione più utile e più informazioni su come raggiungere gli obiettivi. Qualora i TI e RT Providers decidano di collaborare maggiormente durante il test, devono concordare le modalità di lavoro e di condivisione delle informazioni.

Durante la fase di test, si raccomanda che il WT e il RT Provider concordino una modalità regolare di monitorare i progressi del test, ad esempio attraverso aggiornamenti di stato settimanali (es. incontri settimanali); in qualsiasi caso le vulnerabilità potenzialmente critiche e altri problemi di sicurezza devono essere segnalati senza indugio.

Il WT può fermare il test in qualsiasi momento, nel qual caso il RT deve interrompere immediatamente tutte le sue attività di test.

3.5.3 Esecuzione del test di *Red teaming*

L'esecuzione del test TIBER-IT deve essere calibrata in base alla complessità del test stesso. Tenendo conto della natura dinamica e in evoluzione delle minacce, per lo sviluppo degli scenari di attacco, si raccomanda che il TTI *Report* sia utilizzato in un breve lasso di tempo.

Durante il periodo di esecuzione del test il RT Provider dovrebbe svolgere le attività di *red teaming* sui sistemi obiettivo, secondo un approccio guidato dall'analisi della minaccia e cercando di rimanere "invisibile". Il RT Provider può deviare dagli scenari di attacco previsti all'interno del *Red Team Test Plan*, in quanto è un'attività che necessita di creatività (come nei reali attacchi cyber) specialmente in caso di eventuali ostacoli, al fine di sviluppare modi alternativi e sofisticati per raggiungere gli obiettivi del test o catturare le *flags* (es. Scenario X).

Come già accennato, durante la fase di test il RT Provider 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. In tali casi, il WT e il TTM possono concordare di guidare il RT Provider o di dargli un aiuto (*legs-up*), es. fornendo accesso ai sistemi, alla rete interna, ecc. per continuare il test e concentrarsi sulla *flag* successiva. Tutti gli aiuti devono essere debitamente documentati e riportati nel *Red Team Test Report*.

Durante l'esecuzione del test TIBER-IT, il RT Provider dovrebbe aggiornare il TTM almeno una volta alla settimana e tenere il WT informato sui progressi su base continuativa. In questa fase, incontri tra il WT, il TTM, il RT Provider ed eventualmente il TI Provider sono fortemente incoraggiati, in quanto la qualità del test beneficia significativamente dalle interazioni, che aiutano anche a costruire un rapporto di fiducia tra le parti interessate. In ogni caso, tali riunioni devono essere organizzate, condotte e mantenute riservate in quanto il BT deve rimanere all'oscuro del test in corso.

Indipendentemente dalla metodologia utilizzata dal RT Provider, il test è condotto in modo controllato, adottando un approccio graduale e senza mettere a rischio l'entità e le sue FC.

È fondamentale che il RT Provider informi continuamente il WT e il TTM sui progressi compiuti in ogni fase, non appena una *flag* o un obiettivo è in procinto di essere completato o almeno quando il RT Provider ha "catturato la bandiera" (*capture the flag*). Ciò dà al WT l'opportunità di discutere con il RT Provider e il TTM quali passi possano e non possano essere intrapresi in seguito. Inoltre, è il momento in cui si valuta se le procedure di escalation debbano essere attivate. Come già accennato, il WT può interrompere il test in qualsiasi momento, secondo le proprie valutazioni. Tutte le azioni del RT Provider devono essere registrate per la successiva riproduzione con il BT, come evidenza per il *Red Team Test Report*, e per riferimento futuro.

L'output dell'esecuzione del test è una bozza del *Red Team Test Report*[27] prodotto dal RT Provider e da consegnare all'entità. La bozza del report deve essere emanata quanto prima e comunque entro due settimane dal completamento del test, al fine di garantire la qualità stessa del report.

3.6 Fase di chiusura (*closure*)

Nella fase di chiusura dei test TIBER-IT, tutti i soggetti interessati, compreso il BT che è finalmente informato del test, analizzano l'esito del test e apportano i dovuti miglioramenti per rafforzare la resilienza cyber dell'entità sottoposta a test. Questa fase comprende diverse attività, tra cui:

- lo sviluppo del *Red Team Test Report*;
- la stesura del BT *Report*;
- l'esecuzione del *replay workshop* tra RT Provider e BT, possibilmente come *Purple Team*[28] (PT);
- lo svolgimento del *360-degree Feedback Meeting*.

---

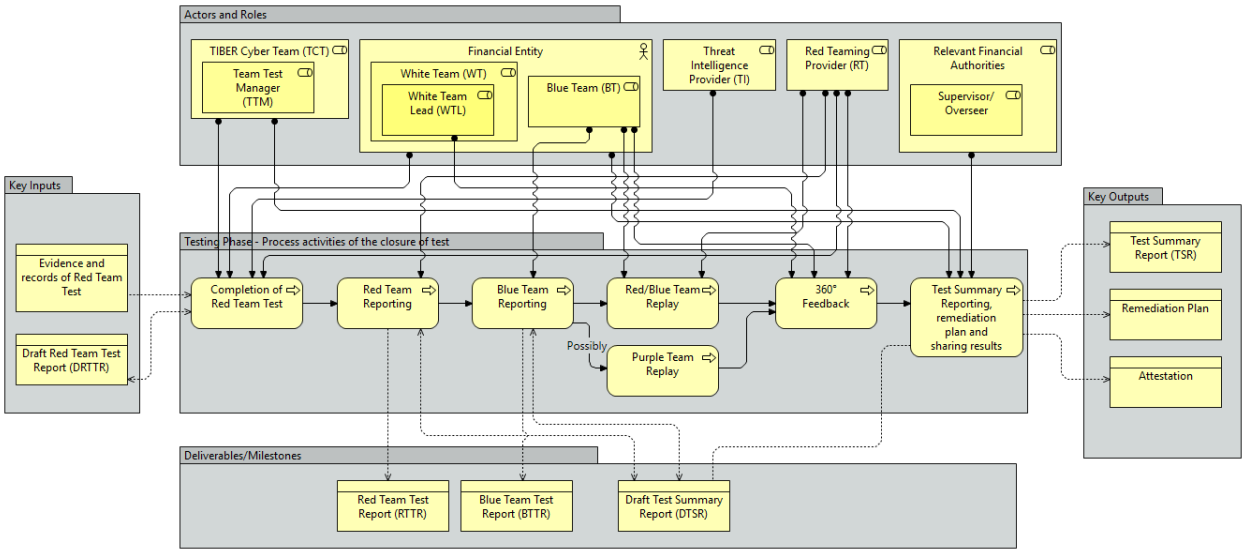
27 https://www.ecb.europa.eu/paym/cyber-resilience/tiber-eu/shared/pdf/final_tiber-eu_guidance-for-the-red-team-test-report.pdf.

28 Il ***Purple Team*** è composto dal BT e dal RT Provider che lavorano insieme per verificare quali altre attività avrebbero potuto essere adottate dal RT Provider e come il BT avrebbe potuto rispondere a tali passaggi. Le TIBER-EU ***Purple Teaming Best Practices*** sono in fase di completamento da parte della BCE in vista della loro pubblicazione sul sito web dedicato al TIBER-EU https://www.ecb.europa.eu/paym/cyber-resilience/tiber-eu/html/index.en.html.

Gli output della fase di chiusura sono: il *Remediation Plan*, il *Test Summary Report* e l'attestazione. Inoltre è compresa anche la condivisione dei risultati con le Autorità competenti.

La fase di chiusura inizia con il completamento del test di *red teaming* ed è seguita dal *replay workshop*, tra il RT Provider e il BT, e dal *360-degree Feedback Meeting*. Successivamente si comunicano i risultati di sintesi del test (*Test Summary Report*), si definisce il piano di rimedio (*Remediation Plan*) e si rilascia l'attestazione del test TIBER-IT (Figura 6).

Figura 6: PANORAMICA DEL PROCESSO TIBER-IT – FASE DI CHIUSURA



In questa fase, il RT Provider redige un *Red Team Test Report*, che include i dettagli dell'approccio adottato per il test e i relativi risultati e le osservazioni. Il rapporto può includere consigli sulle aree da migliorare in termini di politiche e procedure, controlli tecnici, nonché istruzione e sensibilizzazione (*awareness*).

Durante la fase di chiusura, gli scenari di attacco eseguiti durante il test vengono riprodotti dalle parti interessate al fine di analizzare le problematiche emerse. Sulla base dei risultati, l'entità concorda e finalizza, con le autorità competenti (cfr. infra), un *Remediation Plan*, che comprende anche attività di *follow-up*. Inoltre, viene riesaminato l'intero processo di test e vengono analizzate e valutate le capacità dell'entità in termini di rilevamento e risposta. Infine, i principali risultati del test sono condivisi con altre autorità rilevanti.

Le attività svolte durante la fase di chiusura durano circa quattro settimane.

All'inizio della fase di chiusura, il RT Provider produce una bozza del RT *Test Report*, che viene consegnata all'entità. Tale documento, come già menzionato, deve essere rilasciato il più presto possibile ed entro e non oltre le due settimane dalla fine del test.

In questa fase, i membri chiave del BT sono informati del test e si basano sul RT *Test Report* per sviluppare il proprio BT *Report*. Il BT *Report* contiene le azioni

che il BT ha intrapreso durante il test in relazione alle attività del RT Provider. Al fine di massimizzare gli insegnamenti tratti dal *replay workshop*, il BT *Report* dovrebbe essere completato prima della sua data.

Il *replay workshop* tra RT Provider e BT è organizzato dall'entità, dopo la consegna del RT *Test Report* e del BT *Report*. Lo scopo di questo workshop è quello di imparare reciprocamente dall'esperienza del test in collaborazione con il RT Provider. Il *replay* si concentra sull'analisi delle misure adottate dal BT e dal RT Provider durante il test e viene condotto su sistemi di produzione, ove possibile.

Inoltre, in questa fase il BT e il RT Provider possono collaborare come PT, al fine di stabilire quali altri passi avrebbero potuto essere adottati dal RT Provider e in che modo il BT avrebbe potuto rispondere.

Durante il *workshop*, il RT Provider indica quanto sia riuscito a progredire attraverso le fasi di attacco di ogni scenario. Il RT Provider esprime un parere su ciò che si sarebbe potuto ottenere se fosse stato dotato di più tempo e risorse come i reali attori della minaccia.

Il TTM e il TI Provider possono essere presenti anche durante il *replay workshop* tra RT e BT.

Dopo il *workshop*, il TTM organizza un incontro di feedback complessivo (*360-degree Feedback Meeting*) tra il WT, il BT, il TCT e i TI e RT Providers, con l'obiettivo di analizzare congiuntamente il test TIBER-IT per facilitare ulteriormente l'apprendimento di tutti coloro che sono stati coinvolti nel processo in vista di esercitazioni future. Nel corso di questa riunione, tutte le parti interessate dovrebbero reciprocamente fornire il loro feedback su tutti gli altri e sul processo nel suo complesso. In particolare l'agenda di questa riunione include:

- quali attività/risultati sono progrediti adeguatamente;
- quali attività/risultati avrebbero potuto essere migliorati;
- quali aspetti del processo TIBER-IT hanno funzionato correttamente;
- quali aspetti del processo TIBER-IT potrebbero essere migliorati;
- qualsiasi altro feedback.

In tal modo, i TI e RT Providers ottengono un feedback sulle loro prestazioni e le Autorità hanno l'opportunità di migliorare il processo TIBER-IT. Inoltre, un *360-degree Feedback Report* può essere condiviso dal TCT su base anonima con il TKC, per incorporare tutte le lezioni apprese in ulteriori miglioramenti al *framework* TIBER-EU, seguendo il principio del "*learning & evolving*".

Dopo il *replay workshop* tra RT Provider e BT e il *360-degree Feedback Meeting*, l'entità redige un *Remediation Plan* e un rapporto di sintesi del test (*Test Summary Report*).

Il *Remediation Plan* è redatto dal WT con l'avallo del Consiglio di amministrazione dell'entità e consultando i TI e RT Providers; il TTM è informato del piano. Il *Remediation Plan* si basa sui risultati del test e mira ad attuare azioni correttive per mitigare le vulnerabilità individuate.

Il *Test Summary Report*[29] riassume l'intero processo di test e i relativi risultati, e si basa sulla documentazione prodotta durante il processo, come il RT *Test Report*, il BT *Report*, il TTI *Report*, il RT *Test Plan* e il *Remediation Plan*. Il *Test Summary Report* non include informazioni tecniche di dettaglio e risultanze riguardanti le debolezze e le vulnerabilità riscontrate, essendo informazioni altamente sensibili e riservate solo all'entità. Il *Test Summary Report* deve essere condiviso dall'entità con il TCT, che può anche rivedere i risultati più dettagliati del test se lo ritiene necessario.

Al termine della fase di chiusura, una volta concordati i vari report e il *Remediation Plan*, il Consiglio di amministrazione dell'entità e i TI e RT Providers firmano un'attestazione[30] da consegnare al TTM, confermando che il processo di testing è stato condotto conformemente ai requisiti della presente Guida e del *framework* TIBER-EU.

Se vi è stato un accordo per condividere i risultati dei test con altre autorità che non hanno partecipato al test, l'entità o il TCT possono condividere il *Test Summary Report* e l'attestazione.

Al fine di migliorare non solo la resilienza dell'entità sottoposta a test, ma la resilienza dell'intero settore finanziario, il TCT può analizzare i risultati di alto livello di tutti i test (es. il *Test Summary Report*) per identificare le principali problematiche, le aree tematiche, le minacce e le vulnerabilità comuni, e diffonderli nelle forme appropriate alle parti interessate. Il TCT può anche condividere con il TKC e i suoi membri informazioni anonimizzate (ad es. lezioni apprese) relative all'operatività del TIBER-IT. Tali informazioni consentiranno al TKC di aggregare tutte le informazioni più rilevanti per sviluppare una prospettiva globale della resilienza del settore finanziario europeo e apportare miglioramenti ove possibile. In ogni caso, qualsiasi scambio di informazioni dovrebbe avvenire in modo sicuro e protetto.

Il livello di coinvolgimento delle Autorità e delle funzioni di supervisione o sorveglianza è definito dalle Autorità stesse e può anche dipendere dal tipo di entità sottoposta al test. In alcuni casi, una delle Autorità può scegliere di escludere formalmente il coinvolgimento delle funzioni di supervisione o sorveglianza dalla fase di *testing* del TIBER-IT, mentre sarebbero principalmente coinvolte nelle fasi di *scoping* e *closure*. In altri casi, una delle Autorità può scegliere di includere le funzioni di supervisione o sorveglianza in tutto il processo del TIBER-IT. Dopo il completamento del test, l'entità notifica il completamento del test alle proprie Autorità di supervisione e sorveglianza, informando anche il TCT; se le Autorità lo ritengono necessario, l'entità deve condividere il *Test Summary Report* e il *Remediation Plan* con loro. In questa fase, le funzioni di supervisione o sorveglianza possono monitorare le attività svolte dall'entità per implementare le misure di rimedio previste nel *Remediation Plan* del test TIBER-IT.

---

29 https://www.ecb.europa.eu/paym/cyber-resilience/tiber-eu/shared/pdf/final_tiber-eu_guidance-for-the-tiber-eu-test-summary-report.pdf.

30 Il documento da firmare sarà fornito dal TTM, sulla base del template del TIBER-EU: https://www.ecb.europa.eu/paym/cyber-resilience/tiber-eu/shared/pdf/Final_TIBER-EU_Attestation_Template_July_2020.pdf.

4 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* che collaborano al raggiungimento dell'obiettivo comune.

Nella presente Guida sono state descritte tutte le interazioni tra WT e TCT/TTM, così come la stretta cooperazione tra i TI e RT Providers. Inoltre, se ritenuto necessario e in base alle caratteristiche dell'entità sottoposta a test, il TTM può interagire anche con altre autorità finanziarie nazionali e agenzie di 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. Per proteggere ulteriormente la riservatezza dei dati e delle informazioni, i TI e RT Providers dovrebbero firmare un NDA con l'entità sottoposta a test.

Eventuali significative deviazioni dalla pianificazione iniziale sono discusse con il TTM. 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, vincoli di risorse, ecc. possano essere affrontati tempestivamente.

Gli insegnamenti tratti dall'esecuzione dei test TIBER-IT possono essere condivisi dalle Autorità nei pertinenti forum nazionali e internazionali sulla sicurezza informatica (ad es. TKC, ECRB/CIISI-EU[31], CERTFin, eventi accademici, ecc.), purché i dati siano anonimizzati o forniti in forma aggregata e in nessun caso sia possibile riconoscere l'entità finanziaria sottoposta a test.

31 *Euro Cyber Resilience Board for pan-European Financial Infrastructures e Cyber Information and Intelligence Sharing Initiative.*

5 Interazione con le Autorità di supervisione e sorveglianza

L'implementazione del TIBER-IT mira a fungere da catalizzatore e da stimolo per le entità finanziarie critiche del sistema finanziario italiano al fine di migliorare la loro resilienza cyber contro potenziali minacce cyber reali.

Il TIBER-IT non è da intendersi come strumento obbligatorio di supervisione o sorveglianza, tuttavia il ruolo delle Autorità di supervisione e di sorveglianza nel processo è definito nella presente Guida.

Durante la fase di *scoping*, il TTM e il WT si consultano con le competenti Autorità di supervisione e/o di sorveglianza per verificare che i servizi e le funzioni aziendali considerate critiche dalle Autorità di supervisione e di sorveglianza siano incluse nel perimetro del test.

Spetta alle Autorità definire il ruolo delle funzioni di supervisione e sorveglianza nell'implementazione del TIBER-IT. In alcuni casi, una delle Autorità può scegliere di coinvolgere le funzioni di supervisione e sorveglianza durante l'intero processo di test, mentre in altri casi l'Autorità può scegliere che le funzioni di supervisione di sorveglianza non siano coinvolte nella fase di *testing* condotta dai TI e RT Providers e monitorata dal WT e dal TTM. Le informazioni o la documentazione relative al TIBER-IT riguardanti una specifica entità finanziaria possono non esser condivise con le funzioni di supervisione e di sorveglianza durante il test.

Una volta completato il processo del test TIBER-IT, l'entità finanziaria notifica il completamento del test alle Autorità di supervisione e di sorveglianza, informando anche il TCT; se le Autorità lo ritengono necessario, l'entità deve condividere con loro il *Test Summary Report* e il *Remediation Plan*. L'entità sottoposta a test dovrebbe indirizzare i risultati del test e le relative azioni di rimedio nell'ambito delle ordinarie attività informative di supervisione e sorveglianza.

Allegati

Allegato I: matrice RACI del TIBER-IT e principali risultati

Tabella 1: MATRICE DI ASSEGNAZIONE DELLE RESPONSABILITÀ PER UN TEST TIBER-IT

	Fase	Responsible	Accountable	Consulted	Informed	Documentazione
Preparation	Pre-launch	TTM	TTM	WT	TCT	Guida nazionale TIBER-IT Documentazione TIBER-EU
	Procurement	WT	Consiglio di amministrazione dell'entità	TTM	TI e RT Providers TCT	TIBER-EU Service Procurement Guidelines Accordi contrattuali con TI e RT Providers
	Pre-test risk assessment	WT	Consiglio di amministrazione dell'entità	TTM	TI e RT Providers	Pre-test risk assessment report
	Scoping	WT	Consiglio di amministrazione dell'entità	TTM Autorità finanziarie di regolamentazione e supervisione	TI e RT Providers TCT	TIBER-IT Scope Specification Document
	Launch	WT	Consiglio di amministrazione dell'entità	TTM	TI e RT Providers TCT	TIBER-IT Project Plan
Testing: threat intelligence	Fornitura del GTL Report per il settore finanziario	TCT	TCT	Eventualmente Agenzie nazionale di intelligence o di sicurezza Altre Autorità, consulenti e/o TI Providers, CSIRT nazionale e settoriale (e.g. CERTFin)	Autorità e/o settore finanziario	GTL Report
	Targeted Threat Intelligence	TI Provider	WT	TTM RT Provider Eventualmente Agenzie nazionale di intelligence o di sicurezza Altre Autorità, consulenti e/o TI Providers, CSIRT nazionale e settoriale (e.g. CERTFin)	TCT	Targeted Threat Intelligence Report (TTIR)
Testing: test di red teaming	Handover tra TI e RT Providers	TI Provider	WT	RT Providers TTM	TCT	Targeted Threat Intelligence Report (TTIR)
	Sviluppo del Red Team Test Plan e degli scenari di attacco	RT Provider	WT	WT TTM TI Provider	TCT	Red Teaming Test Plan (RTTP)
	Esecuzione del test	RT Provider	WT	WT TTM TI Provider	TCT	Evidenze e registri del test di red teaming Draft Red Team Test Report (DRTTR)
	Riunioni o aggiornamenti regolari sul test	WT	Consiglio di amministrazione dell'entità	RT Provider TTM	TCT	N/A
	Discussioni al momento della cattura delle flags o della necessità di aiuti (*legs-up*)	RT Provider	WT	WT TTM	TCT	N/A
Closure	Produzione del Red Team Test Report	RT Provider	WT	Responsabile per la cyber resilience presso l'entità	TTM TCT	Red Team Test Report (RTTR)
	Sviluppo del Blue Team Report	BT	WT	RT Provider	TTM TCT	Blue Team Test Report (BTTR)
	Red/Blue Team Replay workshop (eventualmente come Purple Team)	WT	Consiglio di amministrazione dell'entità	TI e RT Providers BT	TTM TCT	N/A
	360-degree Feedback meeting	TTM	TTM	WT BT TI e RT Providers	TCT	360-degree Feedback Report (360° FR)
	Redazione del Test Summary Report	WT	Consiglio di amministrazione dell'entità	TI e RT Providers TTM	TCT Autorità finanziarie di regolamentazione e supervisione Altre Autorità rilevanti	Test Summary Report (TSR)
	Remediation plan	WT	Consiglio di amministrazione dell'entità	TI e RT Providers BT TTM	TCT Autorità finanziarie di regolamentazione e supervisione	Remediation Plan
	Firma dell'attestazione del test TIBER-IT	Consiglio di amministrazione dell'entità TI e RT Providers	Consiglio di amministrazione dell'entità	WT TTM	TCT TIBER-IT Steering Committee Altre Autorità rilevanti	TIBER-IT Test Attestation

Allegato II: documentazione TIBER-IT e principali riunioni

Il presente documento, "Guida nazionale TIBER-IT v.1.0", definisce gli elementi fondamentali del TIBER-IT per le Autorità finanziarie italiane, le entità finanziarie, i TI e RT Providers e tutti gli altri soggetti interessati.

Per l'attuazione del TIBER-IT, 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.

Vi sono anche alcuni documenti che devono essere prodotti dall'entità, dalle Autorità, dai TI e RT Providers e/o da altri soggetti interessati per facilitare il processo di test complessivo come riportato nell'allegato 11.3 del *framework* TIBER-EU.

Di seguito sono riportati gli elenchi dei documenti pertinenti e delle principali riunioni previsti dalla presente Guida. Ulteriori informazioni possono essere richieste a tiber-it@bancaditalia.it.

Tabella 2: DOCUMENTAZIONE TIBER-IT

	Documentazione	Titolare della responsabilità
1	Guida nazionale TIBER-IT	Le Autorità che recepiscono il TIBER-IT
3	TIBER-IT *Generic Threat Landscape report (GTL Report)*	TCT
4	TIBER-IT *Test Project Plan*	WT
5	TIBER-IT *Scope specification document*	WT
6	*Targeted Threat Intelligence Report*	TI Provider
7	*Red Team Test Plan*	RT Provider
8	*Red Team Test Report*	RT Provider
9	*Blue Team Test Report*	BT
10	*360-degree Feedback Report*	TTM, TCT
11	*Test Summary Report*	WT
12	*Remediation Plan*	WT
13	TIBER-IT Attestation	Consiglio di amministrazione dell'entità, TI e RT Providers

Tabella 3: PRINCIPALI RIUNIONI TIBER-IT

	Riunioni	Parti coinvolte
1	*Pre-launch meeting*	TTM, WT
2	*Launch meeting*	TTM, WT, TI e RT Providers, altre parti interessate
3	*Scoping meeting*	WT, TTM, TI e RT Providers, altre parti interessate
4	Riunioni settimanali o aggiornamenti sul test	TTM, WT, BT, TI e RT Providers
5	*360-degree Feedback meeting*	TTM, TCT, WT, BT, TI e RT Providers

Glossario

BT	*Blue Team*
CERTFin	*Computer Emergency Response Team* per il settore finanziario italiano
CIISI-EU	*Pan-european Cyber Information and Intelligence Sharing Initiative*
ECRB	*Euro Cyber Resilience Board for pan-European Financial Infrastructures*
FC	Funzioni Critiche
GTL	*Generic Threat Landscape*
NDA	*Accordo di riservatezza (Non-Disclosure Agreement)*
PT	*Purple Team*
RACI	Matrice di assegnazione delle responsabilità (RACI sta per *Responsible, Accountable, Consulted, Informed*)
REDFin	Progetto europeo – *Readiness Enhancement to Defend Financial sector*
RT	*Red Team*
TCT	TIBER *Cyber Team*
TIBER	*Threat Intelligence-Based Ethical Red Teaming*
TI	*Threat Intelligence*
TKC	TIBER-EU *Knowledge Centre*
TTI	*Targeted Threat Intelligence*
TTM	*Team Test Manager*
TTPs	Tattiche, Tecniche e Procedure (Tactics, Techniques and Procedures)
WT	*White Team*
WTL	*White Team Lead*

Indice delle figure e tabelle