Approfondimenti

Gennaio 2019

La "resilienza cibernetica" delle infrastrutture del mercato finanziario

Gian Luca Greco, Università degli Studi di Milano; Federico Bonardi, Trainee Lawyer, Atrigna e Partners Studio Legale Associato

1. Introduzione

Negli anni successivi alla crisi finanziaria mondiale del 2007-2009 i *regulators* hanno più volte insistito sulla necessità, da parte degli intermediari finanziari, di rafforzare la resilienza finanziaria[1], intesa come la capacità di reagire e recuperare rapidamente da *shock* esogeni ed endogeni.

La resilienza cibernetica contribuisce alla resilienza operativa delle infrastrutture del mercato finanziario, a sua volta essenziale per conservare e promuovere la stabilità finanziaria e la crescita economica[2]. Resilienza cibernetica e resilienza finanziaria sono quindi legate in un rapporto di mezzo a fine, in modo particolare per quel che riguarda le infrastrutture del mercato finanziario, visto il ruolo cruciale dalle stesse assunto nelle attività di *clearing*, *settlement* e contabilizzazione delle operazioni monetarie e finanziarie.

Il 3 dicembre 2018 la Banca Centrale Europea (in seguito anche "BCE") ha pubblicato le "*Cyber resilience oversight expectations for financial market infrastructures*" (di seguito, "CROEs")[3]. Tale documento, che definisce le aspettative di vigilanza dell'Eurosistema in termini di resilienza cibernetica nelle infrastrutture del mercato finanziario, è stato adottato in seguito alla pubblica consultazione svoltasi tra aprile e giugno 2018, nel contesto della quale sono pervenuti alla BCE le osservazioni di venti soggetti (tra infrastrutture del mercato finanziario, banche, comunità e associazioni bancarie) rispetto al documento oggetto della consultazione medesima[4].

---

[1] Cfr. M. Draghi, *Strengthening financial resilience*, 2013 International Monetary Conference, Shanghai, 3 June 2013.

[2] CPMI-IOSCO (June 2016), "*Guidance on cyber resilience for financial market infrastructures*", p. 1.

[3] https://www.ecb.europa.eu/paym/pdf/cons/cyberresilience/cyber_resilience_oversight_expectations_for_FMIs.pdf.

[4] Cfr. European Central Bank, "*Response to the public consultation on the cyber resilience oversight expectations – cyber resilience oversight expectations: outcome of the public consultation*", consultabile sul sito *web* della Banca Centrale Europea all'indirizzo www.ebc.europa.eu/home/html/index.en.html.

L'impulso all'*iter* che ha portato alla pubblicazione delle CROEs è costituito dalla pubblicazione della "*Guidance on cyber resilience for financial market infrastructures*", avvenuta nel giugno 2016, da parte del *Committee on Payment and Market Infrastructures* (in seguito anche "CPMI") e del *Board* della *International Organization of Securities Commissions* (in seguito anche "IOSCO"), la quale individua la cornice entro cui le CROEs devono essere sistematicamente collocate[5].

La *Guidance*, a sua volta, costituisce il supplemento dei cc.dd. "PFMIs", ossia i "*Principles for financial market infrastructures*" (in seguito anche solo "*Principles*"), pubblicati nell'aprile del 2012 dal *Committee on Payment and Settlement System* della *Bank of International Settlements* e dal *Technical Committee* dello IOSCO, adottati dal Consiglio Direttivo della BCE il 3 giugno 2013 al fine di indirizzare la vigilanza su tutte le tipologie di infrastrutture del mercato finanziario dell'Eurosistema[6].

Gli scopi precipui delle CROEs sono tre: *«(i) supportare le infrastrutture finanziarie con indicazioni dettagliate su come rendere operativa la* Guidance*; (ii) fornire alle autorità di sorveglianza uno strumento di valutazione delle capacità di* cyber resilience *delle infrastrutture finanziarie sorvegliate; (iii) realizzare una base comune di confronto per una proficua e continua interazione tra le autorità e i soggetti regolati»*[7].

2. Ambito oggettivo

Risulta in primo luogo opportuno definire cosa si intenda per "*cyber resilience*". In proposito soccorrono all'interprete le CROEs medesime, con l'Allegato n. 3 del documento, che contiene un Glossario di riferimento di cui avvalersi per comprendere i concetti ed i termini utilizzati.

Per resilienza cibernetica si intende la capacità di un'organizzazione di continuare a svolgere la propria attività, anticipando ed adattandosi alle minacce cibernetiche nonché ad altri rilevanti mutamenti ambientali, attraverso la comprensione, il contenimento ed il recupero dagli incidenti cibernetici[8].

---

[5] CPMI-IOSCO (June 2016), "*Guidance on cyber resilience for financial market infrastructures*".
[6] CPSS-IOSCO (April 2012), "*Principles for financial market infrastructures*".
[7] Sito *web* di Banca d'Italia, http://www.bancaditalia.it/media/notizia/la-bce-pubblica-la-versione-definitiva-del-documento-cyber-resilience-oversight-expectations/. Cfr. anche il sito *web* della Banca Centrale Europea per la versione in lingua inglese.
[8] Alcune delle definizioni contenute nel Glossario di cui all'Allegato n. 3 sono una trasposizione o un adattamento delle stesse contenute in altre fonti. In particolare, il concetto di resilienza cibernetica è stato adattato dal *Computer Emergency Responce Team Glossary (definition of "Operational resilience")*, dalla *CPMI-IOSCO Guidance* e dal *National Institute of Standards and Technology (definition of "Resilience")/FSB Cyber Lexicon*. Allo stesso modo il termine "*cyber*", ai sensi del Glossario, è identificato come il *quid* "*Relating to, within, or through the medium of the interconnected information infrastructure of interactions among persons, processes, data, and information systems"*.

Per meglio comprendere il significato attribuito al sintagma "resilienza cibernetica" si rende necessaria l'analisi di altri due concetti alla base della definizione stessa: la minaccia cibernetica e l'incidente cibernetico.

a) la minaccia cibernetica è definita come la circostanza che può sfruttare una o più vulnerabilità e che sia idonea ad impattare negativamente sulla sicurezza cibernetica. Le vulnerabilità a cui si fa riferimento sono quelle debolezze o falle in un *asset* o controllo che possono essere sfruttate da una o più minacce, dove per *asset* si intende un *quid* dal valore tangibile o intangibile meritevole di protezione, come persone, informazioni, infrastrutture, finanziamenti e reputazione.

   La sicurezza cibernetica, invece, consiste nella preservazione della riservatezza, dell'integrità e della disponibilità di informazioni e/o di sistemi informativi, attraverso un *medium* cibernetico; in aggiunta, possono essere coinvolte altre proprietà come l'autenticità, l'*accountability*, la non disconoscibilità e l'affidabilità.

b) L'incidente cibernetico è definito come quell'evento cibernetico che, a prescindere dalla circostanza che derivi da attività ostili o meno: *(i)* compromette la sicurezza cibernetica di un sistema informativo o le informazioni che il sistema processa, archivia o trasmette o; *(ii)* vìola le *policy* di sicurezza, le procedure di sicurezza o le regole di utilizzo accettabile delle *policy*.

   Nel contesto della presente definizione, nonché delle CROEs, per evento cibernetico si intende ogni accadimento osservabile in un sistema informativo: si tenga conto che, a seconda dei casi, gli eventi cibernetici possono essere indicatori di un incidente cibernetico in atto[9].

3. Ambito soggettivo

Dopo aver identificato il concetto di resilienza cibernetica utilizzato nelle CROEs, alla luce degli obiettivi perseguiti dal documento medesimo, occorre individuare i soggetti destinatari di tali aspettative di vigilanza.

L'obbligo di resilienza cibernetica grava espressamente sulle infrastrutture del mercato finanziario (*financial market infrastructures* o "FMIs"). Tali sono, secondo la *Guidance*, i sistemi multilaterali tra istituti partecipanti, compreso l'operatore del sistema, che sono utilizzati allo scopo di compensare, regolare o contabilizzare i pagamenti, i titoli, i derivati o altre transazioni finanziarie[10].

[9] I concetti a cui si è fatto riferimento sono definiti singolarmente nell'Allegato n. 3 delle CROEs.
[10] L'Allegato A della *Guidance* contiene un Glossario di riferimento per la stessa, il quale definisce un'infrastruttura del mercato finanziario (o FMI) come "*A multilateral system among partecipating institutions, including the operator of the system, used for the purposes of clearing, settling or recording payments, securities, derivatives or other financial transactions*".

Rispetto a tali soggetti, già identificati come destinatari degli obblighi in commento dalla G*uidance* e, ancor prima, dai *Principles*, il Consiglio direttivo della BCE ha deciso di aggiungere i sistemi di pagamento e il c.d. TARGET2-*Securities* (in seguito anche "T2S")[11]. I sistemi di pagamento includono i SIPSs (*systemically important payment systems*), i PIRPSs (*prominently important retail payment systems*) e gli ORPSs (*other retail payment systems*).

Sempre in tema di soggetti destinatari delle previsioni delle CROEs il punto 1.3 del documento ricorda che, nonostante la vigilanza sui sistemi di pagamento e sul T2S sia di competenza dell'Eurosistema, la vigilanza sui sistemi di compensazione e regolamento[12], in molti paesi dell'area euro, è svolta dalle banche centrali nazionali in base alle proprie competenze, in cooperazione con altre autorità nazionali; in considerazione di ciò, le banche centrali nazionali (e le altre autorità che con esse cooperano) potrebbero optare per avvalersi delle CROEs anche rispetto a queste infrastrutture del mercato finanziario, tenendo conto delle leggi e della regolamentazione in concreto applicabili, al fine di raggiungere i risultati voluti.

4. Le aspettative di vigilanza

4.1. I livelli di aspettative

Le CROEs nascono dalla consapevolezza che il panorama delle minacce cibernetiche è in continua evoluzione e raggiunge via via livelli di sofisticazione sempre più elevati.

Per fronteggiare questa continua evoluzione, le CROEs hanno predisposto tre "livelli di aspettative" che forniscono ai soggetti deputati alla vigilanza (ed ai destinatari della stessa) un *benchmark* rispetto al quale possono: *a)* valutare il livello attuale di resilienza cibernetica delle infrastrutture del mercato finanziario; *b)* misurarne i progressi e; *c)* stabilire quali siano le aree che necessitano di implementazione in via prioritaria[13]. Tali

[11] Il T2S è definito sul sito *web* della Banca d'Italia, che riporta quanto segue: *«Insieme ai sistemi di regolamento all'ingrosso, i sistemi di regolamento dei titoli costituiscono le fondamenta sulle quali poggia la struttura finanziaria delle economie moderne. Questi sistemi consentono infatti lo scambio degli strumenti finanziari e del loro controvalore monetario tra gli operatori. Sistemi di regolamento sicuri ed efficienti costituiscono la premessa per il buon funzionamento dei mercati: in particolare, in un'area valutaria integrata, al fine di garantire la possibilità di investire alle stesse condizioni in tutti i mercati, il regolamento transfrontaliero degli strumenti finanziari deve avvenire a condizioni equivalenti al regolamento domestico. In linea con questo obiettivo, l'Eurosistema ha realizzato TARGET2-Securities (T2S), la piattaforma paneuropea multivalutaria per il regolamento delle transazioni in titoli in moneta di banca centrale. Oggi con T2S le transazioni in titoli sono regolate agli stessi costi e con le stesse modalità in tutti i mercati nazionali dell'Unione Europea, indipendentemente dal paese d'origine dell'investitore»*.

[12] Tra i sistemi di compensazione e regolamento le CROEs fanno riferimento agli SSSs (*securities settlement systems*), ai CSDs (*central securities depositories*) e alle CCPs (*central counterparties*).

[13] Cfr. in proposito il punto 1.4.1 delle CROEs, le quali si occupano di individuare e definire i tre livelli delle aspettative sulla base. Il miglioramento e la maturazione continua da parte delle FMIs costituisce l'essenza dei tre livelli di aspettative; gli stessi, infatti, non sono immaginati per imporre requisiti statici o uno stadio finale di resilienza cibernetica. Tale modo di pensare porterebbe con sé il rischio di creare una "cultura della *compliance*" che sarebbe fuorviante nell'ambito degli obiettivi di resilienza cibernetica.

livelli di aspettative sono denominati rispettivamente "*evolving*", "*advancing*" e "*innovating*"; essi sono rappresentati graficamente in modo piramidale nel documento[14].

I tre livelli di aspettative sono di seguito descritti, premettendo che il termine "capacità" utilizzato *infra* si riferisce alle persone, ai processi e alle tecnologie che l'infrastruttura del mercato finanziario utilizza per identificare, mitigare e gestire i rischi cibernetici che la riguardano, nonché per conseguire gli obiettivi che le sono propri:

a) *evolving*: in questa fase sono predisposte le capacità essenziali; esse si sviluppano e sono mantenute all'interno dell'infrastruttura del mercato finanziario affinché sia possibile identificare, gestire e mitigare i rischi cibernetici, allineandosi a quanto approvato dal *Board* nel contesto della definizione della strategia e del *framework* in materia di resilienza cibernetica[15]. Viene inoltre monitorata e gestita l'esecuzione delle procedure;

b) *advancing*: oltre a dover raggiungere i requisiti posti dal livello *evolving*, le procedure, a questo livello, comprendono l'implementazione di strumenti più avanzati (quali tecnologie avanzate e strumenti di gestione dei rischi) che devono essere incorporati all'interno delle linee operative dell'infrastruttura del mercato finanziario, le quali devono essere migliorate nel tempo per gestire in modo proattivo i rischi cibernetici gravanti sull'infrastruttura stessa;

c) *innovating*: in aggiunta al raggiungimento dei livelli precedenti, le capacità all'interno dell'infrastruttura del mercato finanziario vengono migliorate quanto serve per rispondere alla rapida evoluzione del panorama delle minacce cibernetiche, con l'obiettivo di rafforzare la resilienza cibernetica dell'infrastruttura e del suo ecosistema, collaborando proattivamente anche con i suoi partecipanti esterni.

Questo livello comprende la promozione dell'innovazione rispetto alle persone, ai processi e alle tecnologie dell'infrastruttura del mercato finanziario e del suo più ampio ecosistema, al fine di gestire i rischi cibernetici e di migliorare la resilienza cibernetica. Ciò potrebbe richiedere lo sviluppo di nuovi strumenti e controlli o la creazione di nuovi gruppi per la condivisione delle informazioni.

4.2. Modalità di applicazione delle aspettative

[14] La base di tale struttura piramidale è data dal livello c.d. "*evolving*" mentre l'apice è rappresentato dal livello c.d. "*innovating*".

[15] Ai sensi del Glossario di cui all'Allegato n. 3 delle CROEs (i) la strategia di resilienza cibernetica consiste nell'insieme dei principi e delle pianificazioni a medio termine dell'infrastruttura del mercato finanziario per raggiungere gli obiettivi di gestione dei rischi cibernetici suoi propri e; (ii) il *framework* in materia di resilienza cibernetica consiste nelle *policies*, nelle procedure e nei controlli che un'infrastruttura ha predisposto per identificare, proteggersi, individuare, reagire e riprendersi rispetto alla fonti plausibili di rischi cibernetici che affronta.

Le CROEs forniscono alle infrastrutture del mercato finanziario indicazioni dettagliate e specifiche sulle aspettative di vigilanza per rendere operativa la *Guidance*.

In considerazione del timore manifestato dai partecipanti alla consultazione rispetto ad un possibile eccesso di cogenza delle aspettative, oltre ad aver adottato il principio del *meet or explain*[16], le CROEs specificano che le stesse presentano un grado di flessibilità che consente di tener conto del panorama eterogeneo delle infrastrutture del mercato finanziario, le quali si distinguono le une dalle altre per dimensioni, volume e valore delle transazioni e per il ruolo che svolgono all'interno del sistema finanziario.

In particolare, la funzione di vigilanza dell'Eurosistema si aspetta che tutti i PIRPSs e gli ORPSs raggiungano e mantengano il livello *evolving* (come livello minimo), aggiungendo che l'operatore dovrà nel tempo effettuare dei passi in avanti al fine di raggiungere il livello *advancing*, ove ciò sia ritenuto appropriato. Per quanto riguarda invece i SIPSs e il T2S, essi dovranno raggiungere e mantenere il livello *advancing* e l'operatore dovrà nel tempo effettuare dei passi in avanti per raggiungere il livello *innovating*, ove ciò sia ritenuto appropriato[17].

La *Guidance* ha individuato otto categorie rispetto alle quali le aspettative contenute nei tre livelli devono essere implementate. Una volta raggiunto un livello, le FMIs dovranno continuare a svilupparsi in modo da raggiungere quelli successivi, ove ciò risulti essere in linea con le specificità del proprio *business*; tale processo si svolgerà in un arco di tempo prolungato e parametrato alle criticità della singola infrastruttura attraverso il dialogo tra quest'ultima e i soggetti deputati alla vigilanza di riferimento.

I tre livelli sono pensati per consentire alle FMIs di migliorare le proprie capacità in modo multi-stratificato, lungo un arco di tempo prolungato, affinché ogni livello costruisca e, al tempo stesso, rafforzi le procedure.

5. Le categorie oggetto delle aspettative di vigilanza

La *Guidance*, e conseguentemente le CROEs, sono costruite intorno a otto categorie predeterminate, che vengono in considerazione nella predisposizione di un idoneo

[16] Cfr. il punto 2.1 del "*Response to the public consultation on the cyber resilience oversight expectations – Cyber resilience oversight expectations: outcome of the public consultation*".

[17] Cfr. il punto 1.4.2 delle CROEs, il quale aggiunge che, in ogni caso, il documento non dovrebbe essere considerato come un elenco di misure rispetto alle quali le infrastrutture del mercato finanziario devono essere conformi. Tali misure, piuttosto, dovrebbero prendere in considerazione l'idea di ricomprendere un *set* di procedure che aiutino le infrastrutture ad essere conformi alla *Guidance*. Saranno infatti i soggetti deputati alla vigilanza a giudicare se una FMI, rispetto alle sue criticità, raggiunga i tre livelli delle aspettative; tale giudizio sarà effettuato sulla base di taluni indici quali: *(i)* la cornice legale e regolamentare applicabile in concreto alla FMI; *(ii)* il grado di conoscenza storica di quest'ultima da parte dell'Autorità di vigilanza; *(iii)* la sua dimensione, le sue criticità e il suo modello di *business* e; *(iv)* le discussioni in atto tra i supervisori e l'infrastruttura.

apparato di resilienza cibernetica. In particolare, la *Guidance* distingue cinque categorie primarie di gestione del rischio cibernetico e tre componenti circostanti:

a) le categorie di gestione del rischio cibernetico sono: (i) la *governance*; (ii) l'identificazione; (iii) la protezione; (iv) l'individuazione e; (v) la risposta e la ripresa;

b) le tre componenti circostanti sono: (i) il *testing*; (ii) la consapevolezza del contesto e; (iii) l'apprendimento e l'evoluzione.

5.1. La governance

Col termine *governance* cibernetica si fa riferimento agli accorgimenti che le infrastrutture del mercato finanziario pongono in essere per costituire, implementare e revisionare i propri approcci alla gestione dei rischi cibernetici. Una *governance* effettiva dovrebbe partire da un *framework* in materia di resilienza cibernetica chiaro e completo, che dia priorità alla sicurezza e all'efficienza delle operazioni dell'infrastruttura e che miri al raggiungimento di obiettivi di stabilità finanziaria.

Tale *framework* deve prendere le mosse dalla strategia di resilienza cibernetica e dovrebbe definire in che modo vengono determinati gli obiettivi della FMI in materia; il medesimo quadro deve inoltre evidenziare le persone, i processi e i requisiti tecnologici per la gestione dei rischi cibernetici e per le comunicazioni tempestive, al fine di consentire all'infrastruttura del mercato finanziario di cooperare con i partecipanti rilevanti nella risposta e nella ripresa dagli attacchi cibernetici.

Risulta essenziale che il *framework* sia corroborato da una chiara definizione di ruoli e responsabilità del *Board* dell'infrastruttura, nonché del suo *management*: grava su questi ultimi, infatti, il compito di creare una cultura per la quale si riconosca che lo *staff*, ad ogni livello, ha importanti responsabilità nel garantire la resilienza cibernetica.

Una *governance* cibernetica sviluppata è essenziale per l'implementazione di un approccio sistematico e proattivo nella gestione delle minacce cibernetiche esistenti ed emergenti che vengono di volta in volta affrontate. Essa, da un lato, sostiene gli sforzi svolti nel prendere in considerazione e gestire i rischi cibernetici, dall'altro, fornisce risorse ed *expertise* per affrontarli[18].

5.2. L'identificazione

L'identificazione delle operazioni e degli *asset* informativi che devono essere protetti da possibili compromissioni risulta essere fondamentale per garantire la stabilità finanziaria, la quale potrebbe subire l'impatto negativo di un ipotetico "fallimento nell'operatività". A tal proposito è evidente che la capacità di comprendere le situazioni interne e le

[18] Sul tema della *cyber governance* v. il punto 2.1 delle COREs.

interdipendenze esterne risulti essere un elemento chiave per una risposta efficace a potenziali minacce cibernetiche che potrebbero presentarsi.

Presupposto imprescindibile al riguardo è che una FMI conosca i suoi *asset* informativi e che comprenda i suoi processi, procedure, sistemi e interdipendenze, al fine di rafforzare la sua posizione in materia di resilienza cibernetica[19].

5.3. La protezione

La resilienza cibernetica dipende da controlli di sicurezza efficaci, nonché da sistemi e processi costruiti in modo tale da proteggere la riservatezza, l'integrità e la disponibilità degli *asset* e dei servizi delle infrastrutture del mercato finanziario. Tali misure dovrebbero essere proporzionate al panorama delle minacce e del ruolo sistemico nel sistema finanziario; esse dovrebbero inoltre essere coerenti con la tolleranza ai rischi della FMI[20].

5.4. L'individuazione

Per quanto riguarda l'individuazione, essa consiste nella capacità dell'infrastruttura di riconoscere i sintomi di un potenziale incidente cibernetico o di individuare che è in atto un attacco riuscito. Una individuazione tempestiva, da un lato, fornisce alla FMI un lasso di tempo utile per approntare delle contromisure ad un potenziale attacco, dall'altro, permette un intervento di contenimento proattivo rispetto ad attacchi che hanno già avuto successo. In ultima istanza, un contenimento tempestivo potrebbe comunque mitigare l'impatto dell'attacco.

Considerati la furtività ed il grado di sofisticazione degli attacchi cibernetici, nonché l'esistenza di molteplici punti di ingresso attraverso i quali si potrebbe verificare una compromissione, le infrastrutture del mercato finanziario dovrebbero mantenere capacità efficaci per monitorare in modo estensivo eventuali attività anomale[21].

5.5. La risposta e la ripresa

La stabilità finanziaria potrebbe dipendere dalla capacità di regolamento a scadenze regolari delle obbligazioni da parte delle infrastrutture del mercato finanziario. Ciò considerato, quindi, gli accorgimenti adottati dalle stesse dovrebbero essere pensati e costituiti in modo tale da consentire di riprendere lo svolgimento di operazioni critiche rapidamente, in modo sicuro e con dati accurati, al fine di mitigare potenziali rischi sistemici o il rischio di impossibilità nel regolare tali obbligazioni nel momento in cui i

[19] Per una panoramica completa sulle aspettative di vigilanza riguardanti l'identificazione si veda il punto 2.2 delle CROEs.
[20] La tematica della protezione è affrontata al punto 2.3 delle CROEs.
[21] Per l'analisi dei tre livelli delle aspettative rispetto alla categoria dell'individuazione si veda il punto 2.4 delle CROEs.

partecipanti si aspettano che ciò sia fatto. Una pianificazione nel *continuum* risulta essenziale per raggiungere tali obiettivi[22].

5.6. Testing

Il *testing* è una componente integrante di qualsiasi *framework* avente ad oggetto la resilienza cibernetica. Tutti i singoli elementi di tale cornice, infatti, dovrebbero essere sottoposti a *test* rigorosi per determinare la loro efficacia complessiva; tale adempimento deve essere svolto sia prima che gli elementi in parola siano implementati all'interno dell'infrastruttura, sia successivamente.

Tale adempimento si estende anche alla corretta implementazione, in modo tale che gli elementi del *framework* dipanino i propri effetti in coerenza con gli *output* desiderati.

La comprensione dell'efficacia complessiva del *framework* all'interno dell'infrastruttura del mercato finanziario e del suo ambiente è essenziale per l'individuazione dei rischi cibernetici che residuano rispetto alle operazioni, agli *asset* e all'ecosistema della FMI.

Un regime di *testing* di buon livello produce delle risultanze che vengono utilizzate per individuare eventuali *gap* rispetto agli obiettivi di resilienza prefissati; esso fornisce inoltre *input* credibili e significativi rispetto alle modalità attraverso cui eventuali debolezze e falle nella resilienza cibernetica; in aggiunta, consente di ridurre o eliminare i *gap* identificati.

Il *testing*, ai sensi della *Guidance*, comprende valutazioni sulle vulnerabilità, *test* basati su scenari ipotetici, *test* di penetrabilità e *test* basati sull'utilizzo dei c.d. "*red teams*"[23].

5.7. La consapevolezza del contesto

Il concetto di consapevolezza del contesto si riferisce alla comprensione, da parte dell'infrastruttura del mercato finanziario, dell'ambiente e delle minacce cibernetiche in cui la stessa opera, nonché alle implicazioni derivanti dall'appartenere a tale ambiente in base al proprio *business* e all'adeguatezza delle proprie misure di mitigazione dei rischi cibernetici. Una forte consapevolezza del contesto, acquisita tramite un processo di *cyber intelligence* effettivo, può fare una significativa differenza rispetto alla capacità di un'infrastruttura di prevenire eventi cibernetici o di rispondere rapidamente ed in modo efficace agli stessi. Nello specifico, un ragionato apprezzamento del panorama delle minacce può aiutare l'infrastruttura del mercato finanziario, da un lato, a comprendere meglio le vulnerabilità nelle proprie funzioni di *business* critiche e, dall'altro, a facilitare

[22] Per quanto concerne la risposta e la ripresa v. punto 2.5 delle CROEs.

[23] Si rinvia al punto 2.6 delle CROEs per quanto riguarda i dettagli sulle singole aspettative di vigilanza rispetto al *testing*. Per quanto riguarda i *test* condotti attraverso i *red teams*, essi sono definiti nel Glossario delle CROEs come tentativi controllati di compromettere la resilienza cibernetica di un soggetto, simulando le tattiche, le tecniche e le procedure dei potenziali attori in grado di porre in essere una minaccia cibernetica reale. Tali *test* si basano su *threat intelligence* bersaglio e si concentrano sulle persone, i processi e le tecnologie con un impatto minimo (e noto *ex ante*) sulle operazioni coinvolte.

l'adozione di strategie di mitigazione dei rischi appropriate. In tal modo si consente alla FMI di convalidare la propria direzione strategica, l'allocazione delle risorse, i processi, le procedure ed i controlli, in coerenza con la predisposizione della propria resilienza cibernetica. Una modalità chiave per raggiungere la consapevolezza del contesto da parte di una FMI e del suo ecosistema è la partecipazione attiva della stessa in accordi di condivisione delle informazioni e di collaborazione con partecipanti fidati all'interno e all'esterno del settore industriale di riferimento[24].

5.8. L'apprendimento e l'evoluzione

Il *framework* deve continuamente raggiungere la resilienza cibernetica, anche nel contesto di eventuali mutamenti nell'ambiente delle minacce cibernetiche. Affinché tale quadro sia efficace nel mantenersi in linea con l'evoluzione delle minacce cibernetiche, un'infrastruttura dovrebbe implementare una cornice capace di adattarsi e di evolversi in conseguenza della natura dinamica dei rischi cibernetici; esso, inoltre, deve consentire alla FMI di identificare, valutare e gestire le minacce alla sicurezza e alle vulnerabilità al fine di poter integrare il proprio sistema con strumenti di salvaguardia appropriati.

Una infrastruttura del mercato finanziario dovrebbe avere dunque come obiettivo quello di instillare una cultura della consapevolezza dei rischi cibernetici, in modo tale che lo stato di resilienza, ad ogni livello, sia regolarmente e frequentemente rivalutato[25].

6. La figura dell'Alto Dirigente

Nella parte finale dell'Allegato n. 3, la BCE pone una *Guidance* che prevede e disciplina un soggetto peculiare, il c.d. Alto Dirigente.

In proposito, si stabilisce che le infrastrutture del mercato finanziario debbano provvedere alla sua nomina, che normalmente riguarderà il CISO (*Chief Information Security Officer*), il quale sarà responsabile per le problematiche della FMI e dei terzi coinvolti in materia di resilienza cibernetica.

Il compito precipuo dell'Alto Dirigente è quello di assicurare che gli obiettivi di resilienza cibernetica e le relative misure definite nella strategia della FMI in materia, nonché le *policy* e le linee guida, siano comunicate in modo appropriato sia internamente che, ove ciò risulti opportuno, anche ai terzi; inoltre egli garantisce che la conformità rispetto alle medesime sia monitorata, assicurata e periodicamente rivista.

Più nel dettaglio, è previsto che sull'Alto Dirigente gravino una serie di compiti, elencati nel documento; egli sarà tenuto a:

[24] V. il punto 2.7 delle CROEs.
[25] Ulteriori specificazioni sono contenute nel punto 2.8 delle CROEs.

a) supportare l'alta dirigenza e l'organo di gestione nel definire e aggiornare le *policy* di resilienza cibernetica, fornendo anche consulenza rispetto a tutte le problematiche inerenti alla materia[26];

b) partecipare alla gestione dei rischi cibernetici;

c) produrre le linee guida in materia di resilienza cibernetica e, qualora sia appropriato, ogni altra regola rilevante. Egli deve inoltre verificarne la conformità;

d) influenzare i processi di resilienza cibernetica dell'infrastruttura del mercato finanziario, monitorare il coinvolgimento dei fornitori dei servizi di IT e fornire assistenza rispetto ai relativi compiti;

e) aiutare a produrre e aggiornare il piano di contingenza riguardo ai problemi cibernetici;

f) fornire assistenza e supervisione rispetto all'implementazione delle misure di resilienza cibernetica;

g) partecipare ai progetti rilevanti in materia di resilienza cibernetica[27];

h) svolgere la funzione di punto di contatto per le questioni relative alla resilienza cibernetica che provengono sia dall'interno dell'infrastruttura del mercato finanziario sia da soggetti terzi;

i) indagare sugli incidenti cibernetici e rendicontarli all'alta dirigenza e all'organo di gestione;

j) svolgere sondaggi continui sulle minacce cibernetiche che possono riguardare gli *asset* dell'IT;

k) avviare e coordinare le misure per aumentare la consapevolezza in materia di resilienza cibernetica e per le sessioni di *training*;

l) fornire rendiconti regolari all'alta dirigenza e all'organo di gestione, almeno ogni tre mesi e comunque qualora si renda necessario in considerazione dei eventuali problematiche di resilienza cibernetica[28].

---

[26] Tale attività include anche l'aiuto rispetto alla soluzione di eventuali conflitti tra gli obiettivi prefissati, tra i quali il rapporto costi-benefici e resilienza cibernetica; cfr. sul punto l'Allegato n. 3 delle CROEs.
[27] Ad esempio, monitorando i *test* di sicurezza per le nuove componenti prima che siano immesse nella produzione; cfr. sul punto l'Allegato n. 3.
[28] Il *report* include, per esempio, una valutazione comparata della resilienza cibernetica rispetto al *report* precedente, informazioni sui progetti in materia, sugli incidenti cibernetici occorsi e sui resultati dei *test* di penetrazione e di quelli condotti col metodo dei *red team*.

Per quanto riguarda i requisiti dell'Alto Dirigente, esso deve essere indipendente in modo da evitare ogni possibile conflitto di interessi; per questa ragione, dovrebbero essere adottate talune misure specifiche:

a) predisposizione di misure organizzative che assicurino all'Alto Dirigente o al CISO di agire in modo indipendente rispetto al dipartimento IT (e ai dipartimenti operativi) e che gli consentano di svolgere l'attività di rendicontazione all'alta dirigenza e all'organo di gestione in modo diretto e in qualsiasi momento, garantendo inoltre che l'Alto Dirigente o il CISO non siano convolti in attività della funzione di *internal audit*;

b) determinazione delle risorse necessarie richieste per l'Alto Dirigente o per il CISO;

c) individuazione di un *budget* per le sessioni di *testing* sulla resilienza cibernetica dell'infrastruttura del mercato finanziario e per il *team* o il personale dell'Alto Dirigente o del CISO;

d) identificazione di requisiti in materia di *reporting* dei membri del personale dell'infrastruttura del mercato finanziario e dei fornitori dei servizi IT rispetto agli incidenti rilevanti, secondo una procedura a scalare.

Da ultimo, si sottolinea che ogni FMI dovrebbe avere il proprio Alto Dirigente o CISO interno, qualora ciò sia in linea con la struttura e con l'assetto organizzativo della stessa. Nei limiti previsti dalle discipline nazionali, in caso di gruppo di società è ammissibile la nomina di un CISO di gruppo.