RPLT
RP legalitax

NEWSLETTER

N. 1/2025 del 9 gennaio 2025

Focus: Banca d'Italia. Pubblicate due comunicazioni del 23 e del 30 dicembre 2024 per la corretta attuazione del Regolamento DORA

Banking and finance

HIGHLIGHTS

- Consob. Pubblicate le indicazioni operative per l'applicazione del MiCAR
- Banca d'Italia. Comunicata l'intenzione di volersi conformare agli Orientamenti ESAs sulla cooperazione in materia di sorveglianza e sullo scambio di informazioni tra ESAs e autorità competenti ai sensi del Regolamento DORA
- EBA. Avviata una consultazione sulle RTS relative al calcolo delle esposizioni in *crypto-asset*
- EBA. Pubblicate le *Guidelines* definitive sulla gestione dei rischi ESG

ALTRE NOTIZIE

- Banca d'Italia. Pubblicato un *general framework* su politica monetaria ed euro digitale
- Banca d'Italia. Pubblicate le statistiche aggregate derivanti dal questionario AML

FOCUS

- Banca d'Italia. Pubblicate due comunicazioni del 23 e del 30 dicembre 2024 per la corretta attuazione del Regolamento DORA

HIGHLIGHTS

Consob. Pubblicate le indicazioni operative per l'applicazione del MiCAR

Consob ha pubblicato l'avviso al pubblico del 30 dicembre 2024 con alcune **indicazioni operative** per l'applicazione del Regolamento (UE) 2023/1114 (**MiCAR)**.

Il Regolamento MiCAR, come noto, ha introdotto nell'Unione europea una disciplina armonizzata per:

- l'emissione;
- l'offerta al pubblico; e
- la prestazione di servizi aventi a oggetto cripto-attività non riconducibili a strumenti finanziari o altri prodotti già regolamentati da atti legislativi dell'UE.

In particolare, il MiCAR disciplina l'emissione, la negoziazione e la prestazione di servizi da parte di *crypto asset service provider* (CASP) su tre tipologie di cripto-attività:

- i token collegati ad attività (*asset-referenced token* – "ART"), definiti come cripto-attività che mirano a mantenere un valore stabile facendo riferimento a un altro valore o un diritto o a una combinazione dei due, comprese una o più valute ufficiali;
- i token di moneta elettronica (*e-money token* – "EMT"), definiti come cripto-attività che mirano a mantenere un valore stabile facendo riferimento al valore di una singola valuta ufficiale; e
- le cripto-attività c.d. "*other than*", categoria che ricomprende le cripto-attività diverse dagli ART e dagli EMT; tale categoria include anche gli "*utility token*", ossia le cripto-attività destinate unicamente a fornire l'accesso a un bene o a un servizio prestato dal suo emittente, e le frazioni dei *non-fungible token*, ad esempio quelle emesse in un'ampia serie o raccolta.

Dal **30 dicembre 2024** il MiCAR è direttamente applicabile nella sua interezza e gli operatori sono tenuti alla sua osservanza.

Con la comunicazione Consob n. 1/24 del 12 settembre 2024, al fine di favorire celerità ed efficienza dei processi, i soggetti interessati a presentare alla Consob richieste di autorizzazioni/notifiche sono stati invitati ad avviare interlocuzioni informali e preliminari per ricevere chiarimenti sugli elementi informativi e documentali da allegare alle istanze.

La Nota fornisce, pertanto, **le modalità di contatto della Consob in relazione all'invio delle istanze, delle notifiche e delle comunicazioni** previste dal MiCAR, e individua le sezioni specifiche sul sito Consob per le procedure relative al **trattamento di esposti e segnalazioni di *whistleblowing*** ai sensi rispettivamente degli articoli 108 e 116 del MiCAR.

Link al documento: clicca qui

Banca d'Italia. Comunicata l'intenzione di volersi conformare agli Orientamenti ESAs sulla cooperazione in materia di sorveglianza e sullo scambio di informazioni tra ESAs e autorità competenti ai sensi del Regolamento DORA

La Banca d'Italia, con nota n. 46 del 03 gennaio 2025, ha comunicato all'EBA l'intenzione di volersi conformare entro il 30 aprile 2025 agli Orientamenti congiunti delle ESAs "Orientamenti congiunti sulla cooperazione in materia di sorveglianza e sullo scambio di informazioni tra le ESAs e le autorità competenti ai sensi del Regolamento (UE) 2022/2554 (DORA)" (JC/GL/2024/36).

Il Regolamento DORA introduce, infatti, un quadro di sorveglianza sui fornitori terzi critici ("CTPP" – *Critical Third Party Provider*) di servizi tecnologici della comunicazione e dell'informazione (ICT). Al riguardo, l'articolo 32 descrive la struttura del quadro di sorveglianza, disponendo, al paragrafo 7, l'elaborazione di orientamenti sulla cooperazione tra le ESAs e le autorità competenti concernenti:

- le procedure e le condizioni per la ripartizione e l'esecuzione dei compiti e delle competenze tra le autorità e le ESAs;
- gli scambi informativi necessari per garantire il rispetto delle raccomandazioni rivolte ai fornitori terzi critici di servizi ICT.

Link al documento: clicca qui

EBA. Avviata una consultazione sulle RTS relative al calcolo delle esposizioni in *crypto-asset*

L'EBA ha posto in consultazione una bozza di standard tecnici di regolamentazione (RTS) che specificano gli elementi tecnici necessari agli istituti di credito per calcolare e aggregare le esposizioni in cripto-attività in relazione al trattamento prudenziale.

Tali RTS affronteranno i possibili aspetti di implementazione e garantiranno l'armonizzazione dei requisiti patrimoniali sulle esposizioni in cripto-attività da parte degli istituti in tutta l'UE.

Considerando la rapida evoluzione del mercato delle criptovalute, il Regolamento sui requisiti patrimoniali ("CRR III") ha introdotto un quadro prudenziale transitorio per gli istituti che detengono esposizioni in criptovalute. Le disposizioni considerano i requisiti legali introdotti nel Regolamento sui mercati delle criptovalute ("MiCAR") e specificano, tra gli altri, il trattamento patrimoniale delle esposizioni a token di moneta elettronica ("EMT"), token di riferimento di asset che fanno riferimento a uno o più asset tradizionali ("ART") e altre criptovalute.

La bozza di RTS sviluppa ulteriormente il trattamento patrimoniale pertinente per:

- il rischio di credito;

- il rischio di credito di controparte ('CCR');
- il rischio di mercato ('MR'); e
- il rischio di aggiustamento della valutazione del credito per le esposizioni in criptovalute e in altri cripto-asset.

Le disposizioni transitorie del CRR III, insieme alle norme stabilite nella bozza di RTS, sono state elaborate al fine di consentire agli istituti di credito di capitalizzare adeguatamente le proprie esposizioni in criptovalute fino all'entrata in vigore di un trattamento prudenziale permanente.

La consultazione terminerà **l'8 aprile 2025**.

Link al documento: clicca qui

EBA. Pubblicate le *Guidelines* definitive sulla gestione dei rischi ESG

L'**EBA** ha pubblicato, il 9 gennaio 2024, le linee guida definitive sulla gestione dei rischi ambientali, sociali e di *governance* (ESG) che stabiliscono i requisiti necessari per gli istituti per l'**identificazione, la misurazione, la gestione e il monitoraggio dei rischi ESG**, anche attraverso piani volti ad assicurare la loro resilienza nel breve, medio e lungo termine.

In particolare, tali *Guidelines:*

- specificano i requisiti relativi ai processi interni e alle disposizioni di gestione del rischio ESG che gli istituti dovrebbero adottare in conformità con la Direttiva sui requisiti patrimoniali ("CRD VI");
- specificano il contenuto dei piani che gli istituti devono predisporre al fine di monitorare e affrontare i rischi finanziari derivanti dai fattori ESG, compresi quelli derivanti dal processo di adeguamento verso l'obiettivo di raggiungere la neutralità climatica nell'UE entro il 2050.

Tali piani sosterranno la preparazione degli istituti alla transizione e dovranno essere coerenti con i piani di transizione predisposti o divulgati ai sensi di altri atti legislativi dell'UE.

Le linee guida si applicheranno a partire dall'**11 gennaio 2026**, fatta eccezione per gli istituti piccoli e non complessi, per i quali si applicheranno al più tardi a partire dall'**11 gennaio 2027**.

Link al documento: clicca qui

ALTRE NOTIZIE

Banca d'Italia. Pubblicato un *general framework* su politica monetaria ed euro digitale

La Banca d'Italia ha pubblicato un nuovo numero della collana "Mercati, infrastrutture, sistemi di pagamento", in cui viene proposto un quadro generale per valutare l'ordinata attuazione della politica monetaria, con un *focus* specifico sull'introduzione dell'euro digitale.

Il lavoro propone una metodologia per stimare la quantità massima di euro digitale (D€) che risulti coerente con una ordinata attuazione della politica monetaria nell'area dell'euro (AE).

A tal fine, l'Autorità di vigilanza chiarisce che l'attuazione della politica monetaria potrò essere definita come "ordinata" se, dopo l'introduzione dell'euro digitale:

- la liquidità aggregata rimanente nell'AE sarà sufficiente per ancorare i tassi a breve termine al tasso sulla *deposit facility*; e
- i settori bancari nazionali dell'AE saranno in grado di soddisfare in larga misura la domanda di D€ con l'utilizzo delle riserve in eccesso e un maggiore ricorso al credito di banca centrale.

La Banca d'Italia stima che, per una ordinata attuazione della politica monetaria, la quantità massima di D€ non dovrebbe superare i 1.700 miliardi di euro. Tale risultato tiene conto dell'esistente eterogeneità tra i paesi e le banche nell'AE e della necessità di garantire che nessun sistema bancario nazionale si trovi ad affrontare una crisi di liquidità a seguito dell'introduzione del D€.

Link al documento: clicca qui

Banca d'Italia. Pubblicate le statistiche aggregate derivanti dal questionario AML

Banca d'Italia ha pubblicato le statistiche aggregate su alcune delle variabili acquisite dalle risposte al questionario antiriciclaggio (AML) compilato dagli intermediari nel 2024, e relative all'anno 2023.

A partire dal 2023, la Banca d'Italia valuta l'esposizione ai rischi di riciclaggio e finanziamento del terrorismo (ML/TF) degli intermediari vigilati avvalendosi di nuove metodologie di analisi che utilizzano un ampio insieme di dati, in larga parte forniti dagli stessi intermediari attraverso la compilazione di un questionario, fatto circolare una prima volta nel 2023 e poi nel 2024.

Tali dati, oltre che essenziali per le analisi della vigilanza, possono agevolare gli stessi intermediari nella valutazione dei rischi a cui essi sono esposti.

Link al documento: clicca qui

FOCUS

Banca d'Italia. Pubblicate due comunicazioni del 23 e del 30 dicembre 2024 per la corretta attuazione del Regolamento DORA

La Banca d'Italia ha pubblicato in data 23 dicembre 2024[1] e 30 dicembre 2024[2] due comunicazioni in vista dell'applicazione, **a decorrere dal 17 gennaio 2025**, del Regolamento (UE) 2022/2554 sulla resilienza operativa digitale del settore finanziario (*Digital Operational Resilience Act*) (di seguito il "**Regolamento DORA**").

Il Regolamento DORA è direttamente **applicabile nei confronti delle seguenti entità finanziarie**: banche; istituti di pagamento (IP); prestatori di servizi di informazione sui conti; istituti di moneta elettronica (IMEL); imprese di investimento; fornitori di servizi per le cripto-attività autorizzati (CASP) ed emittenti di token collegati ad attività (ART); depositari centrali di titoli; controparti centrali; sedi di negoziazione; repertori di dati sulle negoziazioni; gestori di fondi di investimento alternativi[3]; società di gestione[4]; fornitori di servizi di comunicazione dati; imprese di assicurazione e di riassicurazione; intermediari assicurativi, intermediari riassicurativi e intermediari assicurativi a titolo accessorio; enti pensionistici aziendali o professionali; agenzie di *rating* del credito; amministratori di indici di riferimento critici; fornitori di servizi di *crowdfunding*; repertori di dati sulle cartolarizzazioni; fornitori terzi di servizi ICT.

Per gli **intermediari finanziari iscritti all'albo di cui all'articolo 106 del TUB**, i quali non sono direttamente ricompresi nel campo di applicazione del Regolamento DORA, la "Legge di delegazione europea 2022-2023" (legge 21 febbraio 2024, n. 15, come emendata dalla legge 28 giugno 2024, n. 90, recante disposizioni in materia di rafforzamento della cybersicurezza nazionale e di reati informatici) ha previsto una specifica delega al Governo per individuare e definire, anche per tali soggetti, presidi in materia di resilienza operativa digitale equivalenti a quelli stabiliti nel Regolamento DORA. Le predette disposizioni dovranno essere adottate dal Governo entro 18 mesi decorrenti dal 10 marzo 2024 (data di entrata in vigore della Legge di delegazione europea 2022-2023), ossia **entro settembre 2025.**

a) Comunicazione della Banca d'Italia del 23 dicembre 2024

Con la prima comunicazione del 23 dicembre 2024, la Banca d'Italia raccomanda agli intermediari da essa direttamente vigilati e destinatari del Regolamento DORA (banche *less significant*, imprese di investimento, gestori[5], istituti di pagamento, istituti di moneta elettronica, emittenti di token collegati ad attività, prestatori di servizi per le cripto-attività, fornitori di servizi di *crowdfunding*) di assicurare il rafforzamento dei presidi del rischio ICT "*che sta ormai travalicando i confini del rischio operativo e assumendo natura trasversale all'intera operatività aziendale, dati il crescente ricorso alla tecnologia e gli impatti che eventuali debolezze nella gestione delle risorse informatiche possono avere sulla reputazione degli intermediari*".

A tal fine, ai predetti intermediari è richiesto di:

---

[1] Comunicazione della Banca d'Italia al mercato in materia di sicurezza ICT: https://www.bancaditalia.it/compiti/vigilanza/avvisi-pub/2024.12.23-com-ict/Comunicazione-ICT.pdf

[2] Comunicazione della Banca d'Italia per l'applicazione del Regolamento DORA: https://www.dirittobancario.it/wp-content/uploads/2024/12/Comunicazione-Banca-dItalia-30-dicembre-2024-sul-Regolamento-DORA.pdf

[3] Un gestore di fondi di investimento alternativi quale definito all'articolo 4, paragrafo 1, lettera b), della direttiva 2011/61/UE, ossia: "*le persone giuridiche che esercitano abitualmente l'attività di gestione di uno o più FIA*" (c.d. GEFIA).

[4] Una società di gestione quale definita all'articolo 2, paragrafo 1, lettera b), della direttiva 2009/65/CE, ossia: "*una società che esercita abitualmente l'attività di gestione di OICVM costituiti in forma di fondi comuni di investimento o di società di investimento (gestione collettiva di portafogli di OICVM)*".

[5] Si ritiene che, in linea con l'ambito di applicazione soggettivo del Regolamento DORA, per gestori si intendano le SGR e le Sicaf e Sicav autogestite.

a) **valutare**, su base consolidata (per i gruppi) e individuale (per i soggetti non appartenenti a gruppi), **il proprio posizionamento rispetto ai requisiti introdotti dal Regolamento DORA**, con particolare riferimento alle seguenti aree: **i)** strategie sul rischio di terza parte, sul rinnovo dei contratti di fornitura e sulla trasmissione all'Autorità del Registro delle Informazioni; **ii)** adattamento di presidi e politiche interne; **iii)** attività e programma di test di resilienza operativa digitale;

b) effettuare **un'autovalutazione del proprio sistema di gestione dei rischi ICT**, al fine di assicurare, in particolare, che le politiche, le procedure, i protocolli e gli strumenti in materia di rischio ICT siano adeguati a: **(i) prevenire, ovvero rilevare tempestivamente, violazioni alla riservatezza dei dati e/o dei servizi forniti**; **(ii) ridurre il rischio derivante dai cambiamenti ICT**.

La comunicazione precisa che il predetto processo di autovalutazione dovrà essere condotto dall'organo di amministrazione dell'intermediario (circostanza che non preclude l'affiancamento di un esperto ICT interno e/o esterno), con il coinvolgimento delle funzioni di controllo di secondo e terzo livello (*risk management*, *compliance* e *internal audit*). **L'esito dell'autovalutazione deve essere trasmesso alla Banca d'Italia entro il 30 aprile 2025**.

Link alla Comunicazione del 23 dicembre 2024 della Banca d'Italia: clicca qui

b) Comunicazione della Banca d'Italia del 30 dicembre 2024

La Banca d'Italia, tenuto conto dell'imminente applicazione del Regolamento DORA, con la Comunicazione del 30 dicembre 2024 ha fornito specifiche precisazioni in merito ai seguenti profili:

1) alla **collocazione della funzione di controllo dei rischi ICT all'interno dell'organizzazione aziendale**, chiarendo che tale funzione deve avere le caratteristiche di una funzione di controllo di secondo livello e che, tra le varie soluzioni organizzative, è ora ammessa l'attribuzione integrale della funzione a una sola delle due funzioni di controllo di secondo livello: alla funzione *compliance* oppure alla funzione *risk management*;

2) all'**esternalizzazione di servizi ICT a supporto di funzioni essenziali e/o importanti** (FEI/FOI), disapplicando taluni procedimenti amministrativi di divieto dell'esternalizzazione da parte della Banca d'Italia e chiarendo, di conseguenza, che a partire dal 17 gennaio 2025, prima di dare corso a eventuali accordi contrattuali previsti per l'utilizzo di servizi ICT a supporto di FEI, gli intermediari sono tenuti a informarne tempestivamente la Banca d'Italia (senza che ciò comporti l'avvio di un procedimento amministrativo);

3) ai ***threat-led penetration test – TLPT*** (test avanzati di test avanzati di penetrazione basati su minacce), che dovranno avere cadenza almeno triennale;

4) alla **segnalazione di gravi incidenti ICT e di minacce informatiche significative**, specificando che a partire dal 17 gennaio 2025 devono essere adottati gli schemi di notifica disciplinati dal Regolamento DORA.

Di seguito si riporta nel dettaglio quanto precisato dalla Banca d'Italia con la comunicazione del 30 dicembre 2024:

1) **Collocazione della funzione di controllo dei rischi ICT**	Ai sensi dell'art. 6, il Regolamento DORA impone alle entità finanziarie di predisporre, monitorare e aggiornare un quadro solido, esaustivo e documentato per la gestione dei rischi informatici. Pertanto, le entità finanziarie, ad eccezione delle microimprese, devono attribuire la responsabilità della gestione dei rischi informatici a una specifica

	"**funzione di controllo ICT**" dotata di un adeguato livello di indipendenza, al fine di evitare possibili conflitti di interesse. Il Regolamento DORA non prescrive regole specifiche sull'organizzazione interna della funzione di controllo ICT, lasciando spazio all'applicazione del criterio della proporzionalità e alla neutralità organizzativa in base ai diversi modelli di *governance* e sistemi di controllo adottati dalle entità finanziarie secondo le discipline settoriali applicabili, opportunamente integrati per tenere conto delle nuove previsioni del Regolamento. In particolare, la Comunicazione precisa che gli intermediari interessati devono adottare una delle seguenti soluzioni alternative: a) **istituire una funzione di controllo ICT autonoma,** prevedendo i medesimi requisiti richiesti alle funzioni aziendali di controllo di **secondo livello**; b) **affidare i compiti** della funzione di controllo ICT **congiuntamente alla funzione di *risk management* e a quella di *compliance***, tenuto conto dei ruoli, delle responsabilità e delle competenze proprie delle due funzioni (qualora la funzione di *risk management* e di *compliance* siano accorpate in un'unica struttura, la funzione di controllo ICT può essere affidata a tale unica funzione di controllo di secondo livello); c) **affidare i compiti** della funzione di controllo ICT **alternativamente alla funzione di *risk management* ovvero alla funzione di *compliance***. **N.B.** Si evidenzia che la soluzione sub lett. c) non è prevista nell'attuale versione della disciplina di vigilanza per le banche di cui alla Circolare della Banca d'Italia n. 285, come modificata dal 40° aggiornamento del 2 novembre 2022 (Parte Prima – Recepimento in Italia della CRD IV, Titolo IV – Governo societario, controlli interni e gestione dei rischi, Capitolo 4 – Il sistema informativo, Sezione II – Governo, organizzazione e controlli del sistema informativo, par. 4.)
2) **Comunicazione all'autorità competente di eventuali accordi contrattuali previsti per l'utilizzo di servizi ICT a supporto di funzioni essenziali o importanti**	Con l'applicazione del Regolamento DORA, le normative settoriali in materia di esternalizzazione ICT non saranno più applicabili. Pertanto, **non sono più applicabili i seguenti procedimenti amministrativi di divieto dell'esternalizzazione previsti dalla normativa secondaria della Banca d'Italia**, ove aventi ad oggetto l'esternalizzazione di servizi ICT a supporto di FEI/FOI:

	(i) divieto di esternalizzare funzioni aziendali operative essenziali o importanti (**Regolamento della Banca d'Italia di attuazione degli articoli 4-undecies e 6, comma 1, lett. b) e c-bis), del TUF: articolo 50, comma 3**); (ii) divieto di esternalizzazione di funzioni aziendali operative essenziali o importanti a fornitori di servizi *cloud* (**Regolamento della Banca d'Italia di attuazione degli articoli 4-undecies e 6, comma 1, lett. b) e c-bis), del TUF: articolo 18, comma 4**); (iii) divieto di esternalizzare, in tutto o in parte, funzioni operative importanti e di controllo a un soggetto esterno o nell'ambito del gruppo di appartenenza per IP e IMEL (**Disposizioni di vigilanza per gli istituti di pagamento e gli istituti di moneta elettronica: Capitolo VI, Sezione II**). **N.B.** I predetti procedimenti amministrativi continueranno invece a trovare applicazione in caso di esternalizzazione di servizi non-ICT. Alla luce di quanto detto, **a partire dal 17 gennaio 2025, in relazione agli accordi di esternalizzazione di servizi ICT, gli intermediari interessati dovranno informare tempestivamente la Banca d'Italia in merito**: a) agli eventuali accordi contrattuali **pianificati** per l'utilizzo di servizi ICT a supporto di funzioni essenziali o importanti (FEI/FOI); b) al momento in cui una funzione già esternalizzata diventa di **carattere essenziale o importante**. A tal riguardo, la Banca d'Italia ha chiarito che le Disposizioni di vigilanza potranno essere modificate, al fine di assicurare il riordino della complessiva disciplina di vigilanza in materia di esternalizzazioni alla luce delle previsioni del Regolamento DORA, in un'ottica di chiarezza del complessivo quadro normativo. Restano, in ogni caso, invariati i poteri di intervento della Banca d'Italia per garantire la sana e prudente gestione degli intermediari, in particolare in relazione a politiche o accordi con i fornitori terzi che potrebbero risultare pregiudizievoli.
3) **Segnalazione dei gravi incidenti ICT e delle minacce informatiche significative**	A partire dal 17 gennaio 2025 entra in vigore il nuovo schema di notifica previsto dal Regolamento DORA e dai relativi atti delegati (RTS e ITS). Pertanto, gli intermediari interessati dovranno:

	a) classificare gli incidenti ICT e le minacce informatiche in conformità a quanto stabilito dal Regolamento delegato (UE) 2024/1772[6]; b) segnalare alla Banca d'Italia gli incidenti ICT utilizzando la rilevazione denominata "DORA – Segnalazione gravi incidenti ICT (DORAI)" e le minacce informatiche significative (su base volontaria) attraverso la rilevazione denominata "DORA – Segnalazione minacce informatiche significative (DORAM)". La segnalazione deve avvenire tramite la piattaforma Infostat e rispettare quanto indicato nell'atto adottato dalla Commissione Europea il 23 ottobre 2024, che ne definisce il contenuto e le tempistiche da rispettare[7]; c) utilizzare, ai fini della segnalazione di cui al punto precedente, il modulo in formato ".xlsx"[8], compilandolo secondo le modalità previste dall'atto adottato dalla Commissione europea il 23 ottobre 2024 che stabilisce i formati, i modelli e le procedure *standard* per la segnalazione dei gravi incidenti ICT e delle minacce informatiche significative.[9]
4) Test avanzati di penetrazione basati sulle minacce (*Threat-Led Penetration Test*)	In ottemperanza di quanto stabilito dall'art. 26 del Regolamento DORA, viene richiesto ad alcune tipologie di intermediari (individuati sulla base di criteri definiti da un apposito atto delegato in corso di adozione) di effettuare test avanzati di penetrazione basati su minacce (*Threat-Led Penetration Test* - TLPT) con cadenza almeno triennale[10]. Per quanto riguarda gli intermediari vigilati direttamente dalla Banca d'Italia, il processo di individuazione degli intermediari interessati è ancora in corso. Una volta concluso, l'Autorità di vigilanza procederà ad informare i soggetti individuati nonché a definire, successivamente, una pianificazione per l'esecuzione dei *test*.

[6] https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=OJ:L_202401772

[7] Regolamento delegato sulle norme tecniche di regolamentazione che specificano il contenuto e i termini della notifica iniziale, della relazione intermedia e della relazione finale per gli incidenti gravi connessi alle TIC nonché il contenuto della notifica volontaria per le minacce informatiche significative: https://webgate.ec.europa.eu/regdel/#/delegatedActs/2503

[8] Disponibile sul sito Internet della Banca d'Italia: https://www.bancaditalia.it/compiti/vigilanza/dora-incidenti/index.html

[9] Regolamento di esecuzione riguardante i formati, i modelli e le procedure standard con cui le entità finanziarie devono segnalare un incidente grave connesso alle TIC e notificare una minaccia informatica significativa: https://ec.europa.eu/transparency/documents-register/detail?ref=C(2024)7277&lang=en

[10] Tale frequenza può essere ridotta o aumentata dalla Banca d'Italia sulla base del profilo di rischio dell'intermediario e tenuto conto delle circostanze operative.

Link alla Comunicazione del 30 dicembre 2024 della Banca d'Italia: **clicca qui**

MILANO
Piazzale Luigi Cadorna, 4
20123 Milano – Italy
+39 02 873131
milano@rplt.it

Piazza Pio XI, 1
20123 Milano – Italy
+39 02 45381201
milano-mi@rplt.it

ROMA
Via Venti Settembre, 98/G
00187 Roma – Italy
+39 06 80913201
roma@rplt.it
roma-rm@rplt.it

TORINO
Via Amedeo Avogadro, 26
10121 Torino – Italy
+39 011 5584111
torino@rplt.it

BOLOGNA
Via D'Azeglio, 19
40123 Bologna – Italy
+39 051 232495
bologna@rplt.it

BUSTO ARSIZIO
Via Goito, 14
21052 Busto Arsizio – Italy
+39 0331 173141
busto@rplt.it

AOSTA
Via Croce di Città, 44
11100 Aosta – Italy
+39 0165 235166
aosta@rplt.it