Circolare n. 285 del 17 dicembre 2013 "Disposizioni di vigilanza per le banche" - 40° aggiornamento.

1. Premessa

Con il presente aggiornamento della Circolare della Banca d'Italia n. 285/2013 sono modificati il Capitolo 4 "Il sistema informativo" e il Capitolo 5 "La continuità operativa" della Parte Prima, Titolo IV, per dare attuazione agli "Orientamenti sulla gestione dei rischi relativi alle tecnologie dell'informazione (ICT) e di sicurezza" (EBA/GL/2019/04) emanati dall'EBA (di seguito "Orientamenti") ([1]), a cui le disposizioni nazionali sono già in larga parte conformi. Con l'occasione sono stati inoltre effettuati alcuni interventi di raccordo e aggiornamento dei riferimenti interni alla Sezione I del Capitolo 3 "Il sistema dei controlli interni" ([2]).

Le modifiche attuano conformemente il contenuto degli Orientamenti dell'EBA. In linea con quanto previsto nel Regolamento della Banca d'Italia sugli atti di natura normativa o di contenuto generale ([3]) non sono state pertanto sottoposte a consultazione pubblica e ad analisi di impatto della regolamentazione (AIR), già svolte a livello europeo.

2. Attuazione degli Orientamenti EBA

Gli Orientamenti definiscono un quadro armonizzato delle misure di gestione dei rischi relativi all'uso delle tecnologie dell'informazione e della comunicazione (ICT) e le misure di sicurezza di cui le banche devono dotarsi. Per la loro attuazione, nel Capitolo 4 sono state modificate le Sezioni I, II, III, IV, VI e VII ed è stata inserita la nuova Sezione IV-bis. È stato inoltre modificato il Capitolo 5.

Il contenuto degli Orientamenti è stato integrato per esteso nel testo delle disposizioni nei casi in cui si è reso necessario coordinarlo con la disciplina vigente; negli altri casi il recepimento è stato effettuato mediante rinvio. In particolare:

i) le previsioni in materia di *governance* e compiti degli organi aziendali, sistema dei controlli interni, esternalizzazione e continuità operativa sono state trasposte per esteso nelle Sezioni I, II e VI del Capitolo 4 e nel Capitolo 5;

ii) le previsioni sulla gestione del rischio ICT e di sicurezza, sulla gestione della sicurezza dell'informazione e delle operazioni ICT, sulla gestione dei progetti e dei cambiamenti ICT, sulla gestione del rapporto con gli utenti dei servizi di pagamento e sulla fornitura di servizi ICT al di fuori dell'esternalizzazione sono state recepite mediante l'inserimento di un rinvio nelle Sezioni III, IV, IV-bis, VI (paragrafo 3) e VII del Capitolo 4.

Tra i principali elementi di novità, le nuove regole prevedono che le banche si dotino di una funzione di controllo di secondo livello per la gestione e il controllo dei rischi ICT e di sicurezza. Le banche possono assegnare la responsabilità di questi compiti a una funzione appositamente costituita, che soddisfi i requisiti previsti dalle norme europee e nazionali per le funzioni aziendali di controllo di secondo livello, assicurando opportuni livelli di raccordo e coordinamento con le altre funzioni aziendali di controllo; in alternativa, le banche possono assegnare tali compiti alle

([1]) EBA *Guidelines on ICT and security risk management*.
([2]) È stato tra l'altro inserito un riferimento esplicito ai rischi ambientali, sociali e di governance (ESG) nell'elenco, non esaustivo, che richiama i principali rischi che le banche devono considerare nell'ambito del processo di gestione dei rischi (cfr. Cap. 3, Sez. I, par. 3, nota 8).
([3]) Provvedimento del 9 luglio 2019 "Regolamento recante la disciplina dell'adozione degli atti di natura normativa o di contenuto generale della Banca d'Italia nell'esercizio delle funzioni di vigilanza, ai sensi dell'articolo 23 della legge 28 dicembre 2005, n. 262, art. 8".

funzioni aziendali di controllo dei rischi e di *compliance*, in relazione ai ruoli, alle responsabilità e alle competenze proprie di ciascuna delle due funzioni, a condizione che siano assicurati il corretto svolgimento dei compiti e le necessarie competenze tecniche e che non si alteri l'efficacia dei controlli sui profili ICT.

3. Procedimenti amministrativi e abrogazioni

Il presente aggiornamento non introduce nuovi procedimenti amministrativi né modifica quelli esistenti.

4. Entrata in vigore

Le disposizioni contenute nel presente aggiornamento entrano in vigore il giorno successivo a quello della pubblicazione sul sito della Banca d'Italia.

Le banche si adeguano al contenuto delle presenti disposizioni entro il 30 giugno 2023. Entro il 1° settembre 2023 trasmettono alla Banca d'Italia una relazione che descrive gli interventi effettuati per assicurare il rispetto delle stesse.

La comunicazione della Banca d'Italia del 12 ottobre 2018 "Misure di sicurezza e presidi di controllo per i servizi informatici esternalizzati o forniti da terze parti" è abrogata dal 1° luglio 2023.

***

Con l'occasione della comunicazione del presente aggiornamento, si informa che a far tempo dal 1° gennaio 2023 la Banca d'Italia non invierà più ai soggetti vigilati le comunicazioni dell'avvenuta pubblicazione sul sito di atti a contenuto normativo o di carattere generale (ad es. disposizioni di vigilanza, chiarimenti interpretativi, orientamenti di vigilanza), dal momento che le forme di pubblicità legalmente previste ne garantiscono la piena conoscibilità e reperibilità. Le banche sono pertanto invitate a mantenere o attivare il sistema di *alert* automatico sul sito web della Banca d'Italia, al fine di ricevere tempestivamente notizia degli atti pubblicati.