RESOCONTO DELLA CONSULTAZIONE

Modifiche alle Disposizioni di vigilanza per le banche. Recepimento degli Orientamenti EBA/GL/2017/10, EBA/GL/2017/17 e delle Raccomandazioni EBA/REC/2017/03

Nella presente tavola sono riportati i nominativi di tutti i soggetti che hanno partecipato alla consultazione e che non abbiano richiesto la non divulgazione.

Rispondenti	• **Associazione Bancaria Italiana – ABI** • **Iccrea Banca S.p.A.** • **Unicredit S.p.A.**

Si riportano di seguito i principali commenti formulati e le relative osservazioni della Banca d'Italia, ripartiti per Titolo/Capitolo e Sezione ed esposti in forma sintetica. I commenti che non hanno ad oggetto le disposizioni secondarie di competenza della Banca d'Italia oggetto della consultazione ("Disposizioni di vigilanza per le banche") non sono riportati.

MODIFICHE ALLE DISPOSIZIONI DI VIGILANZA PER LE BANCHE. RECEPIMENTO DEGLI ORIENTAMENTI EBA/GL/2017/10, EBA/GL/2017/17 E DELLE RACCOMANDAZIONI EBA/REC/2017/03			
ARGOMENTO	OSSERVAZIONE	VALUTAZIONE (Sì/No/In parte/Chiarimento)	COMMENTO
TITOLO IV – Governo societario, controlli interni e gestione dei rischi ***Capitolo 4 – Il sistema informativo***			
Sezione I – Disposizioni di carattere generale	È stato chiesto di allineare le definizioni contenute nella Disposizioni in consultazione e, in particolare, quelle relative a "autenticazione", "autorizzazione" e "credenziali", a quelle di cui all'art. 4 della Direttiva 2015/2366/UE e all'art. 1 del Decreto Legislativo 11/2010 (così come modificato dall'art. 2, comma 1, del Decreto Legislativo 218/2017). L'allineamento è reputato opportuno anche al fine di assicurare continuità nell'applicazione dei requisiti di sicurezza previsti dalle Guidelines	Chiarimento	Le definizioni di "autenticazione", "autorizzazione" e "credenziali" previste dalle Disposizioni hanno carattere generale, perché si riferiscono al sistema informativo aziendale nel suo complesso e non alla sola prestazione di servizi di pagamento. Questa impostazione non interferisce con il rispetto delle indicazioni fornite dall'EBA nella "*Opinion on transition from PSD1 to PSD2*" che prevede la progressiva disapplicazione delle Guidelines EBA in materia di sicurezza dei pagamenti recepite nella Circ. 285, in

	dell'EBA in materia di sicurezza dei pagamenti via internet, secondo quanto previsto dall'EBA nella Opinion on transition from PSD1 to PSD2.		concomitanza con l'adozione dei nuovi requisiti di sicurezza introdotti dalla PSD2 e dai relativi atti attuativi. Ad ogni modo, per favorire la corretta interpretazione delle nome, nelle Disposizioni è precisato che con riferimento alla prestazione di servizi di pagamento restano ferme le definizioni previste dal D. Lgs. n. 11/2010 e dalle altre disposizioni europee direttamente applicabili.
Sezione I – Disposizioni di carattere generale	Con riferimento alla definizione di "grave incidente di sicurezza informatica", è stato proposto di eliminare il riferimento agli incidenti da cui "*[...è probabile che derivi …]*" un impatto negativo, in quanto l'introduzione di una valutazione in termini probabilistici potrebbe portare ad un incremento degli incidenti da segnalare, e di restringere la definizione ai soli incidenti di sicurezza informatica con un "reale impatto".	Chiarimento	La definizione adottata è in linea con quella prevista negli Orientamenti EBA in materia di segnalazione dei gravi incidenti. Come chiarito dall'EBA nel resoconto della consultazione, la comunicazione di incidenti potenzialmente gravi i cui effetti non si sono ancora materializzati ha lo scopo di assicurare la tempestività dell'informativa trasmessa all'autorità competente, nel rispetto di quanto richiesto dalla PSD2. Apposite istruzioni operative della Banca d'Italia, in corso di emanazione, forniranno criteri applicativi che, tra l'altro, agevoleranno l'identificazione dei gravi incidenti da parte degli intermediari.
Sezione IV - La gestione della sicurezza informatica	È stato suggerito di eliminare il riferimento specifico a "*role-based access control*" e di precisare che i diritti di accesso sono accordati sulla base delle *policy* interne tenendo conto dei ruoli e delle responsabilità ricoperte in azienda.	Sì	Testo modificato

Sezione IV - La gestione della sicurezza informatica	In linea con gli Orientamenti EBA sulle misure di sicurezza per i rischi operativi e di sicurezza (EBA/GL/2017/17, Orientamento 4.10), è stato osservato che l'adozione dell' "autenticazione forte" per l'accesso alle componenti critiche del sistema informativo da parte di utenti privilegiati o amministratori di sistema non è richiesta direttamente dagli Orientamenti EBA e potrebbe avere un impatto rilevante sui sistemi informativi degli istituti. È stato pertanto chiesto di modificare le disposizioni per assicurare l'allineamento con le previsioni europee.	Sì	Testo modificato
Sezione IV - La gestione della sicurezza informatica	In materia di conservazione delle tracce elettroniche, si propone di reintrodurre un periodo di conservazione minimo, anche inferiore a quello previsto dalla normativa oggetto di revisione.	No	In linea con quanto previsto dagli Orientamenti EBA sulle misure di sicurezza per i rischi operativi e di sicurezza dei servizi di pagamento, le Disposizioni non prevedono più un periodo minimo di conservazione delle tracce elettroniche. L'obiettivo è valorizzare l'autonomia degli intermediari e incentivare l'individuazione di tempi di conservazione delle tracce elettroniche appropriati in funzione delle caratteristiche delle stesse e dei rischi connessi (c.d. approccio *risk-based*).
Sezione IV - La gestione della sicurezza informatica	È stato proposto di chiarire il rapporto tra gli obblighi di segnalazione dei gravi incidenti previsti dalla Circolare n. 285/Disposizioni di vigilanza per gli istituti di pagamento e di moneta elettronica, dagli Orientamenti EBA/GL/2017/10 e quelli previsti in ambito	Chiarimento	Per quanto concerne gli obblighi di segnalazione degli incidenti previsti dalla Circolare n. 285 e quelli previsti dagli Orientamenti EBA di attuazione di PSD2, la Banca d'Italia ha optato per un'unica procedura di notifica, indipendente dalla tipologia di incidente occorso, che riguarda

	Eurosistema con l'"*Eurosystem major incident reporting framework for payment schemes and retail payment system*" del 7 settembre 2018.		sia servizi di pagamento sia le altre attività e servizi bancari. I nuovi schemi di segnalazione sostituiranno pertanto quelli attualmente utilizzati dalle banche e dagli altri prestatori di servizi di pagamento (cfr. "Comunicazione di gravi incidenti di sicurezza informatica - Banche, Istituti di pagamento, Istituti di moneta elettronica" del 26 giugno 2017, in corso di modifica). Le segnalazioni degli incidenti previste dall' "*Eurosystem major incident reporting framework for payment schemes and retail payment systems"* sono invece oggetto di una distinta procedura di notifica, considerato il differente ambito di applicazione (limitato agli operatori che gestiscono sistemi di pagamento al dettaglio e agli schemi di carte) e le differenti finalità della segnalazione.
Sezione VI – L'esternalizzazione del sistema informativo	È stato suggerito di: (i) sostituire la definizione di *cloud computing* contenuta nelle Disposizioni in consultazione con quelle utilizzate da alcune organizzazioni internazionali (ad es. ENISA, Cloud Alliance, ecc.); e (ii) modificare le definizioni delle tipologie di *cloud* perché, essendo solo di tipo qualitativo, permetterebbero un eccessivo livello di discrezionalità agli operatori.	Chiarimento	Le definizioni di *cloud computing* e delle diverse tipologie di *cloud* (*private*, *community*, *public*, *hybrid*) contenute nelle Disposizioni in consultazione sono in linea con quelle adottate nelle "*Raccomandazioni EBA in materia di esternalizzazione a fornitori di servizi cloud*" (EBA/REC/2017/03) e confermate nelle dalle "*Guidelines on outsourcing arrangements*" (EBA/CP/2018/11) pubblicate lo scorso 25 febbraio 2019.

Sezione VI – L'esternalizzazione del sistema informativo	È stato chiesto di non recepire le Raccomandazioni EBA in materia di esternalizzazione a fornitori di servizi *cloud* (EBA/REC/2017/03) in considerazione della prossima pubblicazione delle "*Guidelines on outsourcing arrangements*" (EBA/CP/2018/11).	No	Le vigenti disposizioni in materia di esternalizzazione dei sistemi informativi prevedono obblighi specifici per le banche che intendono avvalersi di fornitori di servizi *cloud,* già largamente in linea con il contenuto delle Raccomandazioni dell'EBA. Attesa la crescente rilevanza e diffusione del ricorso a fornitori di servizi *cloud*, il recepimento delle Raccomandazioni assicura l'applicazione uniforme di questi obblighi. La circostanza che il contenuto delle Raccomandazioni sia stato trasfuso nelle nuove *Guidelines on outsourcing* non appare sufficiente a posticipare, in assenza di modifiche sostanziali negli obblighi facenti capo agli intermediari, il loro recepimento.
Sezione VII – Principi organizzativi relativi a specifiche attività o profili di rischio.	Nell'ambito degli obblighi in materia di sicurezza dei servizi di pagamento, è stato chiesto di precisare cosa si intende per classificazione delle risorse ICT in termini di "criticità".	Sì	Testo modificato
TITOLO IV – Governo societario, controlli interni e gestione dei rischi ***Capitolo 5 – La continuità operativa***			
Sezione II - **Requisiti per tutti gli operatori**	È stato chiesto di chiarire se le verifiche da effettuare sui piani per la continuità operativa possono essere ricomprese nelle verifiche complessive descritte all'interno del comma 3 del Par. 3.5, Sez. II, Cap. 5.	Sì	Testo modificato
Sezione II -			

Requisiti per tutti gli operatori	È stato chiesto di chiarire come il piano di continuità operativa debba tener conto degli Orientamenti dell'EBA sulla sicurezza dei pagamenti via internet e degli Orientamenti EBA sulle misure di sicurezza per i rischi operativi e di sicurezza; in particolare, è stato chiesto se il piano debba prevedere un "ampliamento dello scenario di crisi" o se invece debba essere adottato un concetto di "indisponibilità del servizio".	Chiarimento	Testo modificato. Al fine di assicurare il coordinamento con gli Orientamenti EBA sulle misure di sicurezza per i rischi operativi e di sicurezza dei servizi di pagamento, le disposizioni precisano che il piano di continuità operativa include, trai fattori di rischio alla base degli scenari presi in considerazione, anche l'indisponibilità dei sistemi funzionali alla prestazione di servizi di pagamento.
Allegato A – Requisiti per la continuità operativa, Sezione I – Disposizioni di carattere generale	È stato richiesto di chiarire il rapporto tra la definizione di *Recovery Time Objective* – RTO contenuta nelle disposizioni in consultazione e quella di cui alle "*Draft Guidelines on ICT and security risk management*" pubblicate da EBA in consultazione il 13 dicembre 2018. Considerato che le banche attualmente utilizzano una definizione già in linea con quella prevista nelle Disposizioni di vigilanza, è stato chiesto se le due definizioni saranno oggetto di allineamento in occasione del recepimento dei citati Orientamenti EBA.	Chiarimento	Le "*Draft Guidelines on ICT and security risk management*" non sono state adottate dall'EBA in via definitiva e sono quindi suscettibili di modifica. Eventuali valutazioni sull'opportunità di modificare la definizione di RTO prevista dalle disposizioni di vigilanza potranno essere effettuate solo una volta che l'EBA avrà emanato il testo definitivo.
Altri aspetti	È stato chiesto di chiarire se, nel recepire gli Orientamenti in materia di misure di sicurezza per i rischi operativi e di sicurezza, si è tenuto in considerazione quanto previsto dalle *Guidelines in ICT and security risk management* poste in consultazione dall'EBA e se sia previsto uno slittamento nel recepimento delle prime.	Chiarimento	Il contenuto delle disposizioni in materia di "Sistema informativo" e "Continuità operativa" è già, in larga parte, coerente con quanto previsto dagli Orientamenti sulle misure di sicurezza per i rischi operativi e per la sicurezza dei servizi di pagamento. Le Disposizioni di vigilanza sono state quindi oggetto di interventi di raccordo tra gli obblighi vigenti, riferiti al complesso delle attività svolte dalla banca, con le specificazioni

			introdotte dagli Orientamenti con riferimento alla prestazione di servizi di pagamento. Le *Guidelines on ICT and security risk management* che l'EBA ha posto in consultazione confermano il contenuto degli obblighi previsti dagli Orientamenti. In assenza di modifiche sostanziali, non si ravvisano quindi ragioni per posticiparne il recepimento. Eventuali interventi di raccordo, potranno essere valutati una volta che l'EBA avrà adottato la versione finale degli Orientamenti.
	È stato chiesto di introdurre un periodo transitorio che consenta agli intermediari di adeguarsi alle nuove disposizioni, con particolare riferimento all'invio della Relazione sulle risultanze dell'analisi dei rischi operativi e di sicurezza relativi ai servizi di pagamento da trasmettersi entro il 30 aprile.	Chiarimento	Non si ritiene di poter accogliere la richiesta di prevedere un regime transitorio in assenza di elementi che ne giustifichino l'introduzione, anche tenuto conto che - come evidenziato nel documento di consultazione - il contenuto delle disposizioni in materia di "Sistema informativo" e "Continuità operativa" applicate dalle banche è già in larga misura coerente con quanto previsto dagli Orientamenti sulle misure di sicurezza per i rischi operativi e per la sicurezza dei servizi di pagamento, che ne rappresentano – di fatto – una specificazione. Quanto Relazione sulle risultanze dell'analisi dei rischi operativi e di sicurezza relativi ai servizi di pagamento, si precisa che le banche sono tenute ad inviare la prima Relazione entro il 30 aprile 2020.