

Scheda informativa - Direttiva sulla Business Continuity per gli istituti finanziari ai sensi dell'art. 17 LIsFi

1. Disposizioni generali

Ogni istituto finanziario deve essere organizzato in modo adeguato ai sensi della Legge sugli istituti finanziari (LIsFi). A tale riguardo, gli organismi di vigilanza e l'Autorità federale di vigilanza sui mercati finanziari (FINMA) verificano che l'istituto finanziario disponga di un sistema di direttive interne che sia completo e adeguato all'attività pianificata e svolta, affrontando tutti i possibili rischi e conflitti, nonché regolamentando gli obblighi ai sensi della LSerFi.

Questa documentazione e identificazione dei rischi operativi includono, in particolare, la regolamentazione della continuità di esercizio in situazioni eccezionali (la c.d. "*Business continuity*"). L'istituto finanziario deve dimostrare che tali situazioni sono definite e che vengono prese o individuate specifiche precauzioni su come la continuità di esercizio possa essere garantita anche in tali circostanze.

La *Business continuity* è intesa come due aspetti: da un lato, deve essere documentato come la continuità delle attività aziendali sia regolata in termini di personale (tramite sistemi di sostituzioni: di solito vengono nominati almeno due persone qualificate incaricate della gestione, oppure un partner esterno cui viene delegata tale attività, etc.). Questo aspetto è solitamente documentato principalmente nelle normative organizzative così come nell'organigramma dell'istituto e di gruppo. D'altra parte, la continuità di esercizio deve essere intesa anche come le precauzioni (infrastrutturali) e organizzative adottate da un istituto per garantire il mantenimento delle operazioni in caso di eventi che complichino o rendano le normali operazioni aziendali più difficili o impossibili (ad esempio guasti dei sistemi IT, pandemia, etc.).

La presente Scheda informativa non pretende di essere esaustiva, ma contiene i punti che di norma devono essere disciplinati e che OSFINcontrol SA considera come contenuto minimo. OSFINcontrol SA verifica il rispetto dei punti menzionati in occasione della verifica di assoggettamento (verifica preliminare) nonché nell'ambito della vigilanza corrente. La concretizzazione delle norme di comportamento – in particolar modo con riguardo alla continuità di esercizio (da un punto di vista del personale – costituisce inoltre un elemento indispensabile per l'autorizzazione da parte dell'Autorità federale di vigilanza sui mercati finanziari).

2. Contenuto della Direttiva

	Temi da regolamentare	Osservazioni
1.	Obiettivi / Basi legali / Destinatari	La direttiva dovrebbe iniziare delineando l'ambito tematico di applicazione. Dovrebbe quindi descrivere cosa si propone di regolamentare: - Definizione di cosa si qualifica come "evento grave" che porti all'attivazione delle misure previste nella direttiva - Consentire ai dipendenti¹ di comprendere e attuare le misure in caso di tali eventi

¹ Per semplicità, in questo opuscolo viene utilizzata la forma maschile. Si intende anche la forma femminile.

		- Regolamentazione delle responsabilità all'interno dell'istituto nel caso in cui si concretizzi uno degli eventi sopra descritti Inoltre, bisogna fare riferimento alle basi rilevanti per la loro applicazione. Infine, si deve indicare a chi si applica la direttiva (di norma a tutti i collaboratori dell'istituto finanziario nonché alla Direzione).
2.	Definizione di eventi e misure associate (catalogo)	La direttiva è intesa a descrivere quali influenze sull'istituto finanziario portano a una situazione particolare per la quale vengono adottate misure e regole su come mantenere le attività aziendali. Gli eventi che hanno tale impatto includono: - Circostanze che rendono impossibile lavorare nell'ufficio (ad esempio danni naturali, incendi, disordini politici, etc.) - Guasto delle telecomunicazioni - Situazioni pandemiche - Problemi di accesso IT - Cyber-attacchi - Altre circostanze In caso di tali eventi, la Direttiva dovrà contenere decisioni approssimative riservate a tali eventi. Deve quindi essere chiaro a ogni dipendente come deve comportarsi – e l'istituto finanziario deve fornire un'infrastruttura (mobile) adeguata per i dipendenti che consenta di continuare le attività aziendali nonostante un evento speciale.
3.	Responsabilità per la gestione delle azioni	È necessario definire chi o quale dipartimento è responsabile, all'interno dell'istituto finanziario, del coordinamento e della gestione delle situazioni che richiedano l'attivazione delle misure di continuità di esercizio. Questo serve a garantire che ci siano linee di reporting e linee guida chiare e che siano fornite a ogni collaboratore istruzioni comprensibili.
4.	Comunicazione	È, inoltre, necessario determinare come garantire la comunicazione interna – specialmente per le unità rilevanti nei rapporti con i clienti – in situazioni eccezionali o di incidenti. Inoltre, deve essere regolamentato in quale misura e in quale forma la comunicazione esterna debba essere effettuata con clienti e terzi riguardo alle strutture e organizzazioni adattate durante tale situazione eccezionale.
5.	Obbligo di documentazione	Quanto segue dovrebbe essere documentato: - Preparazione all'evento - Assicurare / verificare se le misure preparatorie siano (ancora) aggiornate, cioè se siano (ancora) adatte - Chiarimento della responsabilità nei rispettivi eventi - Documentazione di quanto svolto durante la gestione di un evento Documentando l'attuazione delle normative in caso di realizzazione di un "evento", si deve garantire che tutte le attività e interazioni rilevanti per il cliente siano debitamente documentate.