Eidgenössische Finanzmarktaufsicht FINMA
Autorité fédérale de surveillance des marchés financiers FINMA
Autorità federale di vigilanza sui mercati finanziari FINMA
Swiss Financial Market Supervisory Authority FINMA

Comunicazione FINMA sulla vigilanza 04/2024

Gestione dei rischi operativi delle direzioni dei fondi e dei gestori di patrimoni collettivi

12 giugno 2024

Laupenstrasse 27, 3003 Berna, Tel. +41 (0)31 327 91 00, www.finma.ch

Indice

1 Introduzione

Per proteggere in modo efficace gli investitori, le direzioni dei fondi e i gestori di patrimoni collettivi (di seguito: istituti) devono disporre di un sistema di gestione del rischio ben funzionante.

La gestione dei rischi comprende tutti i rischi essenziali, sia a cui l'istituto è o potrebbe essere esposto nell'ambito delle sue attività, sia a livello del patrimonio collettivo da esso gestito e degli altri valori patrimoniali in gestione (cfr. art. 9 e 26 della Legge sugli istituti finanziari [LIsFi; RS *954.1*], art. 12 cpv. 4, artt. 41 e 57 dell'Ordinanza sugli istituti finanziari [OIsFi; RS *954.11*] e art. 8 e segg. e 18 dell'Ordinanza FINMA sugli istituti finanziari [OIsFi-FINMA; RS *954.111*]).

I rischi operativi rientrano tra i rischi essenziali. Come per altri istituti sottoposti alla vigilanza della FINMA, i rischi operativi delle direzioni dei fondi e dei gestori di patrimoni collettivi sono in aumento, come dimostrano in particolare le notifiche di cyber-attacchi. Allo stesso tempo, nelle procedure di autorizzazione e nell'attività di vigilanza, la FINMA constata con frequenza sempre maggiore carenze e punti deboli nella gestione dei rischi operativi da parte delle direzioni dei fondi e dei gestori di patrimoni collettivi.

La presente Comunicazione sulla vigilanza si rivolge pertanto a questi istituti per rammentare loro l'importanza di un'adeguata gestione dei rischi operativi e indicare loro le possibili misure.

In linea con la Circolare FINMA 2023/1 «Rischi operativi e resilienza – banche»[1], il rischio operativo è definito come il pericolo di incorrere in perdite finanziarie dovute all'inadeguatezza o all'inefficacia delle procedure o dei sistemi interni, all'inadeguatezza delle azioni delle persone o a errori da esse commessi oppure causate da eventi esterni. Ciò comprende anche le perdite finanziarie che possono insorgere da rischi giuridici o di *compliance*. La gestione dei rischi operativi deve tenere conto anche di altre dimensioni del danno[2], nella misura in cui esse possano causare tra l'altro perdite finanziarie. Tuttavia, questo concetto non include i rischi strategici.

2 Esempi di carenze e punti deboli identificati

Di seguito sono riportati alcuni esempi di carenze e punti deboli recentemente identificati nell'ambito della gestione dei rischi operativi.

[1] Cfr. www.finma.ch > Documentazione > Circolari.

[2] Per esempio effetti negativi sulla reputazione, possibile perdita di fiducia, perdita di clienti, effetti negativi sul mercato, effetti regolatori negativi (p. es. possibile perdita della licenza).

2.1 Nell’ambito dei processi e delle procedure in generale

L'errata registrazione o l'errata rendicontazione delle transazioni sono state identificate solo dopo l’insorgenza del danno a causa di controlli mancanti o non tempestivi.

2.2 Nel settore delle tecnologie dell’informazione e della comunicazione nonché della sicurezza dei dati

Nell’introduzione di soluzioni cloud per l’archiviazione dei dati dei clienti e aziendali, gli aspetti relativi alla scelta e in particolare al controllo dei fornitori di servizi cloud, ai diritti di accesso, alla sicurezza dei dati e all’inclusione nel *Business Continuity Management* o nei piani di continuità operativa *(Business Continuity Plans)* non sono stati considerati o sono stati considerati in misura insufficiente.

L’identificazione dell’infrastruttura essenziale, in particolare delle tecnologie dell’informazione e della comunicazione, per lo svolgimento delle attività essenziali dell’istituto non è stata effettuata o è stata effettuata in modo lacunoso, motivo per cui per tale infrastruttura non è stata prevista una protezione adeguata e tale protezione non è stata adeguatamente considerata nei piani di continuità operativa.

2.3 Nell’ambito dei cyber-rischi

A causa di attacchi di phishing andati a buon fine, terzi non autorizzati hanno avuto accesso a dati critici di istituti, compresi i dati di accesso alle applicazioni chiave. I dati sottratti sono stati utilizzati in particolare per effettuare transazioni non autorizzate.

Gli istituti che avevano esternalizzato la propria contabilità a un fornitore di servizi esterno hanno temporaneamente perso, in seguito ai cyber-attacchi diretti verso tale fornitore, la visione d’insieme e il controllo della loro situazione finanziaria e quindi la capacità di monitorare la situazione dei fondi propri.

Sebbene gli istituti fossero in grado di rilevare tempestivamente i cyber-attacchi, non disponevano di piani su come rispondere a tali attacchi e come organizzare le responsabilità in questi casi.

Infine, gli istituti non erano a conoscenza dell'obbligo di dover segnalare i cyber-attacchi alla FINMA, come indicato nella Comunicazione FINMA sulla vigilanza 05/2020 «Obbligo di notificare i cyber-attacchi secondo l’art. 29

cpv. 2 LFINMA»[3]. Inoltre, non erano al corrente di dover notificare ogni violazione della sicurezza dei dati all'Incaricato federale della protezione dei dati e della trasparenza[4].

2.4 Nell'ambito del *Business Continuity Management*

I piani elaborati nell'ambito del *Business Continuity Management* (i cosiddetti piani di continuità operativa) non comprendevano tutte le risorse essenziali necessarie per lo svolgimento delle attività essenziali correnti, in particolare in termini di personale e a livello tecnico. Pertanto, non era possibile garantire il mantenimento o la rapida ripresa delle attività essenziali degli istituti in caso di crisi.

I piani di continuità operativa non sono stati testati o non sono stati testati regolarmente, il che ha comportato o potrebbe comportare notevoli ritardi nella riparazione dei danni verificatisi.

2.5 Nell'ambito dei rischi giuridici e di *compliance*

Nella gestione patrimoniale individuale, gli istituti hanno utilizzato strumenti finanziari o applicato tecniche di investimento non adatte ai clienti interessati o non conformi agli accordi.

Gli istituti che fra le altre cose forniscono servizi di gestione patrimoniale per clienti individuali non hanno tenuto sufficientemente conto del domicilio dei clienti target nelle analisi del rischio previste dalla legislazione sul riciclaggio di denaro.

Gli istituti disponevano di una direttiva interna per le attività transfrontaliere e di manuali dei Paesi corrispondenti; tuttavia, i controlli e le responsabilità previsti da questi documenti non sono stati effettuati e rispettati o sono stati effettuati in modo inadeguato.

2.6 Nell'ambito delle attività essenziali esternalizzate

Nella scelta dei fornitori di servizi a cui esternalizzare la gestione del rischio operativo, è stata conferita troppo poca importanza alle conoscenze e all'esperienza di questi fornitori di servizi nell'ambito della gestione dei rischi

[3] Cfr. www.finma.ch > Documentazione > Comunicazioni FINMA sulla vigilanza

[4] Cfr. obbligo di notifica all'Incaricato federale della protezione dei dati e della trasparenza (IFPDT) in caso di violazione della sicurezza dei dati ai sensi dell'art. 24 della Legge federale sulla protezione dei dati (LPD), v. servizio online per la notifica di violazioni della sicurezza dei dati (art. 24 LPD).

operativi (cfr. nm. 16-21 della Circolare FINMA 2018/3 *«Outsourcing»*[5] concernente i requisiti per la scelta, l'istruzione e il controllo dei fornitori di servizi).

Le attività esternalizzate non sono state registrate o non sono state registrate correttamente (cfr. nm.14-15.1 Circ. FINMA 18/3 concernenti l'iscrizione nell'inventario delle funzioni esternalizzate). Ciò ha comportato lacune nei controlli, oppure queste attività esternalizzate sono state incluse in maniera insufficiente nella gestione dei rischi operativi.

3 Requisiti generali relativi alla gestione del rischio

3.1 Gestione del rischio in generale

Per evitare i punti deboli e le lacune summenzionate e simili, la FINMA rammenta pertanto alle direzioni dei fondi e ai gestori di patrimoni collettivi i requisiti generali per un'adeguata gestione del rischio.

L'organo preposto all'alta direzione, alla vigilanza e al controllo fissa nelle direttive interne i principi per la gestione di tutti i rischi essenziali, sia a cui l'istituto è esposto con la sua attività, sia a livello di patrimonio che gestisce. Deve inoltre determinare la tolleranza al rischio.

Sulla base delle disposizioni impartite dall'organo preposto all'alta direzione, alla vigilanza e al controllo, l'organo responsabile della gestione deve adottare direttive, procedure e processi adeguati per l'identificazione, la valutazione, la gestione e il controllo dei rischi. Deve inoltre designare le funzioni o le persone competenti e responsabili e garantire un'adeguata rendicontazione periodica all'attenzione dell'organo preposto all'alta direzione, alla vigilanza e al controllo.

L'organo preposto all'alta direzione, alla vigilanza e al controllo e l'organo responsabile della gestione devono riesaminare regolarmente l'adeguatezza e l'efficacia dei loro principi, della tolleranza al rischio, delle direttive, delle procedure e dei processi per la gestione del rischio, in particolare in caso di modifiche dell'attività o dell'organizzazione.

3.2 Gestione dei rischi operativi come componente della gestione del rischio

I rischi operativi rientrano tra i rischi essenziali delle direzioni dei fondi e dei gestori di patrimoni collettivi, come pure dei patrimoni da essi gestiti. Di con-

[5] Cfr. www.finma.ch > Documentazione > Circolari.

seguenza, i suddetti requisiti si applicano anche alla gestione dei rischi operativi. In particolare, in termini di personale ciò significa che le persone incaricate della gestione dei rischi operativi devono disporre delle conoscenze e delle esperienze necessarie.

4 Gestione dei rischi operativi

4.1 Principi generali per la gestione dei rischi operativi e relativa organizzazione

Una gestione efficace dei rischi operativi a livello di istituto presuppone che vengano considerate le attività effettivamente svolte e l'organizzazione dell'istituto. Al riguardo occorre prestare particolare attenzione alle procedure e ai processi utilizzati per lo svolgimento di queste attività, nonché alle risorse in termine di personale e tecniche impiegate, così come i dati richiesti.

Nell'organizzare i processi e le procedure operative, l'istituto deve prevedere misure e controlli adeguati (p. es. applicando il principio del doppio controllo) per garantirne l'efficacia e l'affidabilità.

4.2 Elementi specifici della gestione dei rischi operativi

4.2.1 Rischi della tecnologia dell'informazione e della comunicazione

La base per una gestione efficace dei rischi legati alle tecnologie dell'informazione e della comunicazione è costituita da un inventario delle principali componenti hardware e software utilizzate dall'istituto nei processi e nelle procedure per lo svolgimento delle sue attività principali.

Per tali componenti l'istituto definisce la tolleranza al rischio e adotta le misure necessarie per garantire la disponibilità, la riservatezza e l'integrità definite.

4.2.2 Rischi relativi ai dati critici

Occorre identificare i dati degni di particolare protezione (p.es. i dati dei clienti) o critici per l'attività dell'istituto e adottare misure di protezione adeguate per garantirne la disponibilità, la riservatezza e l'integrità.

Ciò significa anche che devono essere chiaramente definiti i compiti, le responsabilità e le competenze, nonché i controlli per la gestione dei dati critici.

4.2.3 Cyber-rischi

In base alle sue attività e alla sua organizzazione, un istituto deve analizzare e identificare le potenziali minacce derivanti dai cyber-attacchi. Di conseguenza, adotta misure di protezione adeguate e garantisce il monitoraggio della propria infrastruttura di informazione e comunicazione.

È auspicabile prevedere una regolare formazione e sensibilizzazione del personale in merito alla gestione dei cyber-rischi.

In caso di cyber-attacco riuscito o almeno parzialmente riuscito, l'istituto deve prevedere misure che gli consentano di riprendere tempestivamente il normale esercizio. Deve inoltre assicurarsi di adempiere correttamente l'obbligo di notificare i cyber-attacchi[6].

Soprattutto nella gestione dei cyber-rischi, è importante che l'istituto abbia definito chiaramente i compiti, le competenze e le responsabilità e che tenga conto anche della comunicazione, in particolare con i clienti interessati, i partner commerciali e, se del caso, altre persone.

4.2.4 *Business Continuity Management*

L'istituto deve elaborare un piano di continuità operativa adeguato alle proprie attività e alla propria organizzazione per mantenere e ripristinare i processi e le procedure essenziali per l'esercizio in caso di crisi.

È importante che tale piano venga rivisto periodicamente e, se necessario, aggiornato. È inoltre opportuno rivedere ed eventualmente aggiornare il piano di continuità operativa ogni volta che vengono apportate modifiche alle attività e all'organizzazione.

I piani di continuità operativa devono essere testati periodicamente, soprattutto per gli istituti con attività ampie o complesse.

Infine, è importante che l'istituto disponga di una chiara strategia di comunicazione per le emergenze e che abbia definito chiaramente compiti e competenze.

[6] Cfr. l'obbligo di notificare i cyber-attacchi ai sensi dell'art. 29 cpv. 2 LFINMA e della Comunicazione FINMA sulla vigilanza 05/2020 (cfr. nota 3), nonché l'obbligo di notifica all'Incaricato federale della protezione dei dati e della trasparenza (IFPDT) in caso di violazione della sicurezza dei dati ai sensi dell'art. 24 della Legge federale sulla protezione dei dati (LPD; RS **235.1**) (cfr. nota 4).

4.2.5 Gestione dei rischi giuridici e di *compliance*, in particolare per le attività transfrontaliere

Se un istituto eroga servizi transfrontalieri o distribuisce strumenti finanziari a livello transfrontaliero, deve garantire di rilevare, limitare e sorvegliare adeguatamente i rischi che ne derivano.

L'istituto deve analizzare le proprie attività transfrontaliere e la distribuzione transfrontaliera di strumenti finanziari sotto il profilo del quadro giuridico e dei rischi associati, nonché adottare le misure necessarie per mitigare tali rischi.

La situazione giuridica nei Paesi interessati deve essere costantemente monitorata e, se necessario, le misure adottate per la mitigazione del rischio devono essere adattate.

4.2.6 Gestione dei rischi operativi in caso di esternalizzazione

4.2.6.1 Esternalizzazione della gestione del rischio e della *compliance*

L'istituto deve inoltre garantire che le misure per la gestione dei rischi operativi vengano attuate anche se la gestione del rischio e la *compliance* sono esternalizzate a terzi. Di conseguenza, nella scelta dei terzi a cui affidare la gestione del rischio, l'istituto deve tenere conto anche della loro conoscenza ed esperienza nell'ambito della gestione dei rischi operativi.

4.2.6.2 Esternalizzazione di attività essenziali

Se l'istituto esternalizza a terzi altre attività essenziali per la propria attività o ottiene da terzi le risorse necessarie per processi e sistemi essenziali, deve garantire il rispetto dei requisiti previsti dalla Circ. FINMA 18/3[7] (in particolare per quanto riguarda l'inventario delle funzioni esternalizzate, la scelta, l'istruzione e il controllo del fornitore di servizi). L'istituto deve inoltre garantire che le funzioni esternalizzate siano incluse nella gestione dei rischi operativi.

[7] Cfr. nota 5.