

Legge sulle banche

Ultima modifica: 23.08.2026

PDF creato il: 05.10.2026



COMMENTARIO ONLINE
IL COMMENTARIO GIURIDICO
IN OPEN ACCESS

INDICE

Art. 1b LBCR.....	5
-------------------	---

ATTENZIONE: Questa versione del commentario è una traduzione automatica dell'originale. Il commentario originale è in tedesco. La traduzione è stata effettuata con www.deepl.com. Solo la versione originale fa fede. La forma tradotta del commentario non può essere citata

COMMENTO SU

Art. 1b LBCR

Un commentario di Tamara Teves / David Meirich

CITAZIONE SUGGERITA

Tamara Teves/David Meirich, Commentario all'art. 1b LBCR, in: Nina Reiser/Beat Brändli (a cura di), Commentario online alla legge sulle banche

Breve citazione: OK-Teves/Meirich, art. 1b LBCR N. XXX.

Art. 1b Promovimento dell'innovazione

¹ Le disposizioni della presente legge si applicano per analogia alle persone che operano soprattutto nel settore finanziario e:

- a. accettano a titolo professionale depositi del pubblico per un importo inferiore o pari a 100 milioni di franchi o beni crittografici definiti tali dal Consiglio federale oppure si prestano pubblicamente a tale scopo; e
- b. non investono tali depositi o beni né corrispondono interessi sugli stessi.

² Il Consiglio federale può adeguare l'importo di cui al capoverso 1 tenendo conto della competitività e del potenziale di innovazione della piazza finanziaria svizzera.

³ Le persone di cui al capoverso 1 devono in particolare:

- a. delimitare esattamente la sfera degli affari e prevedere una organizzazione proporzionata all'importanza degli stessi;
- b. disporre di una gestione dei rischi adeguata e di un controllo interno efficace, tali da garantire in particolare il rispetto delle prescrizioni legali e delle direttive interne dell'impresa (conformità alle norme);
- c. disporre di risorse finanziarie adeguate;
- d. assicurare che le persone incaricate dell'amministrazione e gestione godano di buona reputazione e offrano la garanzia di un'attività irreprensibile;

⁴ Sono fatte salve le seguenti disposizioni:

- a. la presentazione dei conti delle persone di cui al capoverso 1 è retta esclusivamente dalle disposizioni del Codice delle obbligazioni (CO);
- b. le persone di cui al capoverso 1 fanno verificare il loro conto annuale ed eventualmente il loro conto di gruppo secondo le disposizioni del CO¹⁴, di cui tuttavia non è applicabile l'articolo 727a capoversi 2–5;
- c. le persone di cui al capoverso 1 incaricano una società di audit abilitata dall'Autorità federale di sorveglianza dei revisori conformemente all'articolo 9a capoverso 1 o 4^{bis} della legge del 16 dicembre 2005 sui revisori di effettuare una verifica conformemente all'articolo 24 della legge del 22 giugno 2007 sulla vigilanza dei mercati finanziari;
- d. ai depositi del pubblico e ai beni crittografici definiti tali dal Consiglio federale detenuti dalle persone di cui al capoverso 1 non si applicano le disposizioni sui depositi privilegiati (art. 37a) e sul pagamento immediato (art. 37b); i depositanti ne vanno informati prima di effettuare il deposito.

⁵ In casi particolari la FINMA può dichiarare applicabili i capoversi 1–4 anche alle persone che accettano a titolo professionale depositi del pubblico per un importo superiore a 100 milioni di franchi, o si prestano pubblicamente per tale scopo, e non investono tali depositi né corrispondono interessi sugli stessi, sempre che la protezione dei clienti sia garantita mediante misure particolari.

⁶ Se il valore soglia di 100 milioni di franchi è superato, ciò va notificato alla FINMA entro 10 giorni; entro 90 giorni va presentata una domanda di autorizzazione secondo l'articolo 1a. È fatto salvo il capoverso 5.

STRUTTURA

I. Introduzione	11
II. Procedura di autorizzazione	12
A. Esame preliminare	12
B. Esame della domanda.....	14
C. Decisione di autorizzazione.....	17
III. Ambito di applicazione (cpv. 1 e 2)	18
A. Accettazione di depositi del pubblico (cpv. 1, lett. a)	18
B. Custodia collettiva di valori patrimoniali basati su criptovalute (cpv. 1, lett. a).....	18
C. Divieto di investimento e di remunerazione (cpv. 1 lett. b)	19
D. Adeguamento della soglia per i depositi del pubblico da parte del Consiglio federale (cpv. 2)	21
IV. Presupposti per l'autorizzazione (cpv. 3 e 4)	21
A. Oggetto sociale (cpv. 3 lett. a).....	21
1. Considerazioni generali	21
2. Custodia di depositi del pubblico e di valori patrimoniali basati su criptovalute (cpv. 3 lett. a)	24
a. Custodia di depositi del pubblico.....	24
b. Monitoraggio della soglia per i depositi del pubblico (cpv. 6)	26
3. Custodia degli attivi basati su criptovalute	27
B. Organizzazione amministrativa adeguata (cpv. 3 lett. a).....	28
1. Forma giuridica, sede e luogo di attività	28
2. Organi	30
3. Infrastruttura e personale	31
a. Locali commerciali.....	31
b. Risorse umane	32
c. Infrastruttura tecnica	32
4. Esternalizzazioni	32
a. Esternalizzabilità	32
b. Rilevanza	33
c. Inventario.....	35
d. Analisi dei rischi	35
e. Selezione, istruzione e controllo del fornitore di servizi	35
f. Revisione e vigilanza	35
g. Contratti di esternalizzazione	36
h. Rendicontazione	37
i. Situazioni relative al gruppo.....	38
j. Responsabilità e sicurezza	38
k. Esternalizzazioni all'estero	38
l. Obblighi e deroghe.....	38

C. Corporate Governance: gestione dei rischi, controlli interni e compliance (cpv. 3 lett. b)	39
1. Principi fondamentali.....	39
2. Funzioni di controllo indipendenti	41
3. Gestione dei rischi	42
a. Competenze	42
b. Inventario	43
c. Identificazione	43
d. Tolleranza al rischio	44
e. Formazione del personale	44
f. Controllo	44
g. Rendicontazione	45
h. Rischi ICT	45
a. Strategia e governance	45
b. Gestione delle modifiche.....	45
c. Gestione delle TIC.....	46
d. Gestione degli incidenti.....	46
i. Rischi informatici	47
j. Rischi relativi ai dati critici.....	49
k. Gestione della continuità operativa.....	50
l. Rischi derivanti dall'attività transfrontaliera di prestazione di servizi.....	51
m. Resilienza operativa	52
4. Ufficio specializzato in materia di riciclaggio di denaro	53
5. Documentazione e processi	54
6. Prevenzione dei conflitti di interesse	55
D. Requisiti finanziari (cpv. 3 lett. c)	55
1. Piano aziendale	55
2. Liquidità	57
3. Capitale minimo	57
E. Garanzia (cpv. 3 lett. d)	58
F. Rendicontazione e revisione contabile (cpv. 4, lettere a, b e c)	61
G. Obblighi di informazione (cpv. 4, lett. d)	62
V. Casi particolari (compresi i cpv. 5 e 6)	63
A. Possibile aumento della soglia per i depositi del pubblico da parte della FINMA (cpv. 5 e 6).....	63
B. Combinazione con altre categorie di autorizzazione	64
C. Vigilanza consolidata.....	64
D. Situazioni transfrontaliere	68
1. Attività all'estero (outbound).....	68
2. Controllo estero.....	69
3. Rappresentanze (inbound).....	70

VI. Modifiche all'autorizzazione..... 71

VII. Cronologia delle autorizzazioni..... 73

VIII. Ulteriore sviluppo dell'autorizzazione nel settore fintech 74

Bibliografia 75

I materiali..... 77

I. INTRODUZIONE

Il presente art. 1b è stato inserito dal Parlamento nella Legge sulle banche (Lb) ¹ il 15 giugno 2018 – nell’ambito delle disposizioni relative alla **promozione dell’innovazione** – insieme alla Legge sui servizi finanziari e alla Legge sugli istituti finanziari. Tutte queste disposizioni relative alla promozione dell’innovazione sono entrate in vigore il 1° gennaio 2019.

Il **settore fintech** è soggetto a continui cambiamenti. Di conseguenza, anche i ² modelli di business in questo ambito sono in continua evoluzione. Per tenere conto di questa circostanza, la categoria di autorizzazione di cui all’art. 1b cpv. 1 dell’LBCR non si limita né a determinati modelli di business fintech né al settore fintech in quanto tale. Sebbene la nuova normativa mirasse principalmente a ridurre gli ostacoli all’ingresso sul mercato per le imprese fintech, la disposizione è formulata in modo aperto e si applica in generale a tutte le persone che operano nel settore finanziario. Pertanto, in linea di principio, anche le imprese al di fuori del settore fintech possono ottenere un’autorizzazione ai sensi dell’art. 1 b della Legge sulle LBCR, purché soddisfino i requisiti di legge. L’ambito di applicazione aperto trova espressione anche nel titolo della disposizione di legge («Promozione dell’innovazione»). Nonostante l’ambito di applicazione aperto, nella pratica l’attenzione si concentra tuttavia sul settore fintech. Nell’ambito di questa categoria di autorizzazione non è tuttavia richiesta una particolare innovazione.

Anche i modelli di business degli istituti fintech richiedono in parte la ³ **raccolta di depositi dal pubblico** (cosiddetta attività di passività). Tuttavia, lo svolgimento concomitante dell’attività di attività (e quindi dell’attività di differenziale di interesse) deve rimanere riservato alle banche anche dopo l’introduzione delle disposizioni sulla promozione dell’innovazione. Per questo motivo, un istituto fintech non è autorizzato a investire o a remunerare con interessi i fondi raccolti (cfr. art. 1b cpv. 1 lett. b LBCR).

Prima dell’emanazione dell’art. 1b LBCR, la raccolta a titolo professionale di ⁴ depositi del pubblico era riservata esclusivamente alle **banche**. L’esercizio di tale attività senza autorizzazione come banca era punibile (cfr. art. 46 cpv. 1 lett. a e art. 49 cpv. 1 lett. c LBCR). Gli istituti fintech, in particolare, che

rientrano in questa normativa forniscono servizi simili a quelli bancari, ma operano al di fuori dell'attività principale delle banche.

- 5 In Svizzera, numerosi servizi (sia servizi di pagamento che negoziazione e custodia individuale di valori patrimoniali basati su criptovalute) – purché la loro attività non sia disciplinata da altre disposizioni della normativa sui mercati finanziari – sono possibili anche senza l'autorizzazione dell'Autorità federale di vigilanza sui mercati finanziari (FINMA), ma sotto la vigilanza in materia di riciclaggio di denaro di un OAD. In questo modo, sotto la vigilanza di un OAD possono essere offerti sia determinati servizi di pagamento sia il commercio e la custodia individuale di criptovalute (attualmente si stima che siano circa 200 i fornitori di servizi di criptovalute e circa 50 i fornitori di servizi di pagamento soggetti alla vigilanza di un OAD). È necessario tenere conto di questo contesto quando si formulano previsioni sul numero di nuovi fornitori di servizi. Il regime di licenze fintech ai sensi dell'art. 1b LBCR si rivolge, in tal senso, a un profilo di modello di business molto specifico: istituti che raccolgono e trasferiscono depositi del pubblico (fondi dei clienti) (servizi di pagamento).
- 6 Il rispetto dei requisiti di autorizzazione è monitorato dalla FINMA nell'ambito di una vigilanza continua; la FINMA è inoltre competente per l'applicazione di sanzioni prudenziali in caso di comportamenti illeciti, quali l'esercizio di un'attività soggetta ad autorizzazione senza averla ottenuta.

II. PROCEDURA DI AUTORIZZAZIONE

A. Esame preliminare

- 7 La FINMA effettua, per i progetti che potrebbero sfociare in una procedura di autorizzazione per istituti fintech (come nel caso delle banche e delle società di intermediazione mobiliare), effettua un esame preliminare. L'**esame preliminare** ha lo scopo di consentire alla FINMA di familiarizzarsi con le linee generali del progetto e di effettuare una prima valutazione della situazione dal punto di vista normativo. In questo modo, i promotori del progetto possono ricevere tempestivamente indicazioni su eventuali ostacoli all'autorizzazione o discutere direttamente con la FINMA questioni per loro fondamentali.

Ai fini di un primo contatto, è necessario presentare alla FINMA una **8 descrizione del progetto** che dovrebbe contenere almeno le seguenti informazioni:

- modello di business e descrizione dell'attività soggetta ad autorizzazione;
- figure chiave del progetto (ovvero le persone coinvolte che, se del caso, ricopriranno in seguito il ruolo di «garanti»);
- dotazione finanziaria del progetto e provenienza dei fondi (sulla base di dati aggiornati);
- organizzazione prevista;
- se il progetto fa parte di un gruppo: panoramica della struttura del gruppo;
- eventuali indicazioni su fatti degni di nota che potrebbero essere rilevanti per la procedura di autorizzazione (ad es. procedimenti a carico di potenziali garanti);
- calendario;
- procura (in caso di rappresentanza).

In sintesi, la presentazione del progetto alla FINMA deve fornire un primo **9** quadro della composizione personale, finanziaria e organizzativa del progetto oggetto di autorizzazione.

Dopo aver ricevuto la presentazione del progetto, la FINMA decide in merito **10** all'opportunità di convocare una seduta. Singole questioni relative al contesto autorizzativo, la cui risposta riveste particolare importanza per la questione principale, possono essere trattate, su richiesta, nell'ambito di una **questione preliminare**. Le presentazioni dei progetti devono essere inviate in una delle lingue ufficiali o in inglese al Fintech-Desk della FINMA.

Se, nell'ambito dell'esame preliminare, la FINMA giunge alla conclusione che **11** la **idoneità all'autorizzazione** del progetto presentato non sia presumibilmente data, ad esempio per mancanza di mezzi finanziari sufficienti, provenienza dei fondi non verificabile, per l'impossibilità di esercitare una vigilanza consolidata, per l'insufficiente qualificazione delle persone coinvolte in qualità di futuri garanti o per l'insufficiente presenza economica in Svizzera, si sconsiglia la presentazione di una domanda di autorizzazione. In tal caso, i promotori del progetto hanno la possibilità di presentare un nuovo progetto preliminare, a condizione che gli aspetti

sollevati durante il colloquio vengano adeguatamente affrontati e che possano essere presentate le relative prove.

- 12 Se la FINMA ritiene che il progetto presentato sia presumibilmente idoneo all'autorizzazione, al richiedente viene comunicata la possibilità di presentare la **domanda di autorizzazione**. La domanda preliminare deve essere semplice ed economica. Di conseguenza, non viene condotta come una procedura amministrativa formale che si conclude con una decisione. Può piuttosto essere intesa come un servizio di chiarimento preliminare fornito dalla FINMA.
- 13 Gli accertamenti relativi ai progetti di autorizzazione sono soggetti a tassa. La **tassa** è stabilita in base all'Ordinanza sulle tasse e sui diritti della FINMA (OTF-FINMA).

B. Esame della domanda

- 14 A seguito di un esame preliminare positivo e in presenza di un rapporto di autorizzazione, la relativa **domanda di autorizzazione** può essere presentata alla FINMA.
- 15 In base al sistema di doppia vigilanza, nella procedura di autorizzazione la FINMA richiede di norma alla richiedente un **rapporto di revisione per l'autorizzazione** redatto da una società di revisione debitamente autorizzata ai sensi dell'art. 9a della LSR. La necessità di tale rapporto va valutata caso per caso; di norma, tuttavia, viene richiesto un rapporto di revisione. I rapporti di revisione delle diverse società di revisione differiscono in parte notevolmente in termini di qualità (approfondimento della revisione) e di costi, aspetto di cui la richiedente deve tenere conto nella scelta. Maggiore è la qualità del rapporto, maggiore è l'utilità del rapporto di revisione nell'ambito dell'ulteriore trattamento della domanda da parte della FINMA. La durata della procedura di autorizzazione dipende infine dalla complessità del progetto, nonché dalla qualità e dalla completezza della domanda.
- 16 Le **linee guida della FINMA** relative alle attestazioni che le società di revisione devono presentare in merito alle domande di autorizzazione come soggetti ai sensi dell'art. 1b della LBCR sono rivolte alle società di revisione in relazione alle domande di autorizzazione presentate da istituti fintech di nuova costituzione. Le linee guida indicano le attestazioni necessarie e gli ambiti di revisione che le società di revisione, in qualità di revisori per

l'autorizzazione, devono almeno coprire nell'ambito di una procedura di autorizzazione. Non escludono che le società di revisione forniscano ulteriori informazioni o che la FINMA richieda ulteriori informazioni e attestazioni.

Qualora venga richiesta una verifica di autorizzazione – cosa di cui di norma si deve presumere – la richiedente deve presentare, insieme alla domanda di autorizzazione, una dichiarazione di accettazione in tal senso da parte della **società di revisione incaricata della verifica**, nonché il questionario compilato relativo ai servizi delle società di revisione autorizzate. 17

La FINMA è competente per il rilascio dell'autorizzazione fintech. In caso di relative domande di autorizzazione, l'autorità di vigilanza valuta se l'attività commerciale prevista sia soggetta ad autorizzazione e se tale attività sia possibile nell'ambito dell'autorizzazione fintech. Al fine di agevolare la procedura di autorizzazione, la FINMA ha pubblicato delle linee guida per i richiedenti. Tali linee guida definiscono in particolare quali documenti devono essere allegati alla domanda. 18

La domanda deve essere redatta in una **lingua ufficiale o in inglese**, mentre lo statuto, il regolamento organizzativo ed eventuali altri documenti di natura societaria soggetti ad approvazione devono essere presentati in una lingua ufficiale svizzera. La FINMA non accetta statuti e regolamenti organizzativi in inglese. Nella pratica, tali documenti di diritto societario vengono di norma redatti in due lingue, cosa che la FINMA ha finora accettato. Se la domanda viene presentata da un rappresentante legale, occorre allegare la relativa procura. 19

Dopo aver ricevuto la domanda, la FINMA comunica al richiedente quale collaboratore della FINMA è responsabile della **procedura di autorizzazione** e quali ulteriori informazioni e documenti devono eventualmente essere presentati in un secondo momento. 20

L'autorità di vigilanza può svolgere autonomamente o far svolgere l'**esame per il rilascio dell'autorizzazione**, come del resto tutti gli altri esami (cfr. art. 24 cpv. 1 della Legge sulla vigilanza sui mercati finanziari [LFINMA] in combinato disposto con l'art. 2 cpv. 2 dell'Ordinanza sulla vigilanza sui mercati finanziari [OP-FINMA]). Si verifica se le disposizioni di vigilanza siano rispettate e se sussistano i presupposti o se questi possano essere soddisfatti in un futuro prevedibile (art. 2 cpv. 1 OP-FINMA). La verifica si concentra in particolare sui rischi che il soggetto sottoposto a vigilanza può comportare per 21

i creditori e per il corretto funzionamento dei mercati finanziari. Ove possibile, occorre evitare duplicazioni nella verifica (art. 24 cpv. 2 LLFINMA).

- 22 La FINMA si assicura in particolare, già nell'ambito dell'esame preliminare, che eventuali **ostacoli fondamentali al rilascio dell'autorizzazione** vengano individuati tempestivamente. Non appena sono disponibili tutte le informazioni e i documenti rilevanti, la FINMA esamina la pratica e decide se l'autorizzazione possa essere concessa. Il richiedente ha l'obbligo di collaborare al completamento del quadro fattuale e alla dimostrazione dei requisiti per il rilascio dell'autorizzazione. L'autorizzazione richiesta viene concessa se tutti i requisiti per il rilascio sono soddisfatti senza ombra di dubbio o possono essere soddisfatti.
- 23 La **durata dell'esame** della domanda di autorizzazione dipende dalla qualità e dalla complessità della stessa, nonché dallo scambio di informazioni con i richiedenti. Nel caso di domande con un riferimento all'estero particolarmente marcato, come ad esempio l'appartenenza a un gruppo con società estere già esistenti nel settore finanziario o il coinvolgimento di persone che in passato sono state segnalate dalle autorità di vigilanza dei mercati finanziari esteri, occorre inoltre tenere conto dei tempi di risposta delle autorità di vigilanza estere competenti.
- 24 **Fattori**, che determinano procedure di autorizzazione prolungate possono anche presentarsi in combinazione tra loro:
- preparazione insufficiente delle domande di autorizzazione (ad es. descrizione non sufficientemente concreta dell'attività prevista, documentazione carente o errata);
 - modifiche alle domande di autorizzazione apportate dai richiedenti durante l'esame in corso da parte della FINMA (ad es. modifica delle attività commerciali previste e/o dell'organizzazione, modifiche dei garanti);
 - numerosi elementi che aumentano la complessità (ad es. garanzie discutibili circa l'irregolarità dell'attività commerciale delle persone rilevanti, precedente rigetto di una domanda di autorizzazione della richiedente da parte di un'autorità di vigilanza estera, provenienza poco chiara dei fondi destinati al finanziamento della società, piani aziendali o di finanziamento palesemente irrealistici).

La FINMA sta attualmente valutando l'introduzione di una «**procedura fast track**» per progetti ben preparati, in cui i rischi siano adeguatamente affrontati, in modo che questi non debbano risentire dell'elevato impiego di risorse destinato alle altre domande di autorizzazione. Ciò mira a evitare che l'impiego di risorse prolunghi i tempi di trattamento anche delle domande di autorizzazione ben preparate e meno complesse. 25

C. Decisione di autorizzazione

La FINMA conclude la procedura di autorizzazione con una **decisione di autorizzazione**. La decisione è suddivisa in esposizione dei fatti, motivazione e dispositivo. Mentre l'esposizione dei fatti descrive l'organizzazione del richiedente, nella motivazione si fa riferimento al soddisfacimento dei requisiti di autorizzazione applicabili nel caso specifico. Nel dispositivo, la FINMA dispone il rilascio dell'autorizzazione, il che avviene di norma con efficacia giuridica sospesa in relazione a oneri e condizioni da adempiere in precedenza. Come tali, gli oneri e le condizioni comprendono di norma la sottoscrizione di contratti di lavoro o di esternalizzazione, l'entrata in vigore di direttive e regolamenti, la disponibilità di un esemplare validamente firmato del regolamento organizzativo e di gestione, nonché la disponibilità degli atti pubblici relativi alla delibera dell'assemblea generale concernente l'adozione del progetto di statuto, la nomina ancora in sospeso dei membri del consiglio di amministrazione e la nomina dell'ufficio di revisione. 26

L'autorizzazione decade di norma, se le condizioni menzionate nel dispositivo della decisione non vengono soddisfatte entro un **termine di un anno** dall'entrata in vigore della decisione e la richiedente non è stata iscritta nel registro di commercio come persona ai sensi dell'art. 1b LBCR. L'autorizzazione decade inoltre se la richiedente non avvia la propria attività commerciale (accettazione di depositi dal pubblico e/o custodia collettiva di valori patrimoniali basati su criptovalute) entro un anno dall'entrata in vigore della presente decisione. Contro la decisione di autorizzazione può essere presentato ricorso dinanzi al Tribunale amministrativo federale entro 30 giorni (art. 54 cpv. 1 LFINMA in combinato disposto con l'art. 33 lett. e della Legge sul LTF. 27

III. AMBITO DI APPLICAZIONE (CPV. 1 E 2)

A. Accettazione di depositi del pubblico (cpv. 1, lett. a)

- 28 Con l'art. 1b della LBCR è stata creata una nuova categoria di autorizzazione per gli istituti che accettano a titolo professionale depositi del pubblico fino a CHF 100 milioni senza esercitare attività di gestione del credito (la cosiddetta «autorizzazione fintech»). I requisiti per l'autorizzazione sono stati precisati dal Consiglio federale nell'ambito di una revisione parziale dell'Ordinanza sulle banche (OB), entrata in vigore il 1° gennaio 2019.

B. Custodia collettiva di valori patrimoniali basati su criptovalute (cpv. 1, lett. a)

- 29 Con l'entrata in vigore della legge federale del 25 settembre 2020 sull'adeguamento del diritto federale agli sviluppi della tecnologia dei registri elettronici distribuiti a partire dal 1° agosto 2021, l'**ambito di applicazione** dell'autorizzazione fintech è stato ampliato.
- 30 Ai sensi dell'art. 1b cpv. 1 lett. a LBCR, da allora rientra nell'ambito dell'autorizzazione fintech anche chi accetta a titolo professionale **valori patrimoniali basati su criptovalute** (in custodia collettiva) designati dal Consiglio federale ai sensi dell'art. 5a dell'Ordinanza sulle banche (OB).
- 31 Gli attivi basati su criptovalute sono attivi in custodia collettiva ai sensi dell'art. 16 cpv. 1^{bis} lett. b della LBCR, che di fatto o secondo l'intenzione dell'organizzatore o dell'emittente servono in misura significativa come mezzo di pagamento per l'acquisto di beni o servizi o per il trasferimento di denaro o valori, ovvero (ibridi) **token di pagamento** (art. 5a cpv. 1 OB).
- 32 Nel caso della **custodia collettiva**, l'istituto fintech è tenuto a tenere a disposizione del cliente i token di pagamento in qualsiasi momento; i token sono assegnati a una comunità ed è possibile verificare (tramite blockchain o sulla base di un registro interno) quale quota del patrimonio comune (ovvero un indirizzo blockchain comune) spetta al rispettivo cliente (art. 16 cpv. 1^{bis} lett. b LBCR).
- 33 La **custodia individuale** dei token di pagamento su un indirizzo blockchain individuale ai sensi dell'art. 16 cpv. 1^{bis} lett. a LBCR non rientra quindi nell'ambito di applicazione dell'autorizzazione fintech. Ciò vale anche per la

custodia di token di utilizzo o di investimento, ovvero token privi di funzione di pagamento (ibrida).

Un'**autorizzazione** ai sensi dell'art. 1b LBCR può quindi essere ottenuta, da un lato, da chi accetta a titolo professionale depositi del pubblico fino a CHF 100 milioni o valori patrimoniali basati su criptovalute designati dal Consiglio federale, oppure raccomanda pubblicamente l'accettazione di tali depositi o valori patrimoniali basati su criptovalute e, dall'altro lato, non investe né remunera tali depositi del pubblico o valori patrimoniali basati su criptovalute. L'autorizzazione viene concessa se sono soddisfatti i requisiti di autorizzazione previsti dal diritto bancario ai sensi dell'art. 1b LBCR. 34

C. Divieto di investimento e di remunerazione (cpv. 1 lett. b)

Il **divieto di investimento e di remunerazione** ai sensi dell'art. 1b cpv. 1 lett. b LBCR comporta di fatto un divieto di concessione di crediti, ovvero un divieto di attività di credito. Rientrano quindi nella categoria di autorizzazione degli istituti fintech solo i modelli di business che rinunciano all'attività di credito. In questi casi, la licenza fintech non prevede la possibilità di svolgere l'attività di differenziale di interesse tipica delle banche. 35

Il concetto di **investimento** va inteso in senso molto ampio. Poiché i fondi non possono essere investiti, si deve presumere che siano mantenuti costantemente liquidi sui conti dell'impresa in questione (cfr. art. 14^f cpv. 2 dell'Ordinanza sulle banche), trasferiti secondo la destinazione prevista dall'accordo con la clientela o – qualora ciò non sia lo scopo o non sia possibile – restituiti alla clientela. Ai titolari di autorizzazione è quindi vietato esercitare l'attività di differenziale di interesse riservata alle banche e generare profitti dalla differenza tra interessi attivi e passivi. Il divieto di investimento implica inoltre che i depositi non possano essere investiti (a proprio nome e per proprio conto) in prodotti di investimento. 36

A tal proposito, il divieto di investimento e di remunerazione comporta nella pratica le seguenti **conseguenze**: 37

- Gli istituti fintech non possono concedere ai propri clienti **alcun credito** finanziato tramite depositi del pubblico. Ciò vieta anche gli scoperti di conto e situazioni simili, nonché il prefinanziamento infragiornaliero delle transazioni dei clienti (ad es. nel settore del cambio valuta o dei pagamenti internazionali) tramite depositi del pubblico. È quindi necessario chiarire,

caso per caso, in che modo i relativi fornitori di servizi terzi fatturino le commissioni di transazione e di tenuta conto, nonché i prefinanziamenti e i margini sulle transazioni, ad esempio se gli importi versati quotidianamente siano finanziati con fondi della società o con depositi del pubblico;

- sono altresì vietati gli **anticipi** a carico dei fondi propri per l'esecuzione delle transazioni dei clienti. Gli anticipi infragiornalieri a carico dei fondi propri per l'esecuzione delle transazioni dei clienti sono ammessi, se del caso, in applicazione dell'eccezione di cui all'art. 5 cpv. 3 lett. a OB;
- **B un istituto fintech** non può, in linea di principio, offrire **B operazioni a termine su valute**, poiché i rischi di capitale e di liquidità ad esse connessi richiederebbero requisiti almeno simili a quelli bancari;
- è possibile trasferire gli **B interessi negativi**, ma non gli interessi positivi sui depositi dei conti correnti presso la BNS;
- i **B prodotti di credito** nel settore delle criptovalute non possono essere offerti con l'autorizzazione fintech;
- **lo staking custodiale** è soggetto all'autorizzazione bancaria, fatte salve le eccezioni di cui agli articoli 5, 5a e 6 dell'Ordinanza sulle banche (OB), nella misura in cui lo staking comporti di fatto una remunerazione (staking rewards), il che sarebbe in contrasto con il divieto di remunerazione; in alternativa, gli Staking Rewards potrebbero anche qualificarsi come commissioni di utilità, per cui lo staking custodito potrebbe essere offerto anche da istituti fintech, a condizione che, per quanto riguarda gli attivi basati su criptovalute oggetto di staking, siano sempre rispettati i requisiti della comunicazione di vigilanza FINMA 08/2023 «Staking». La dottrina nega che vi sia una violazione del divieto di remunerazione nel pagamento degli Staking Rewards ai clienti.
- Le **piattaforme di negoziazione CFD** bilaterali si qualificano in linea di principio come sistemi di negoziazione organizzati (OHS) bilaterali ai sensi della Legge sulle infrastrutture dei mercati finanziari (LInFi). La qualificazione come attività OHS comporta la necessità di un'autorizzazione come banca, società di intermediazione mobiliare, sistema di negoziazione DLT o piazza di negoziazione (borsa, MHS) (art. 43 cpv. 1 LInFi). Un'autorizzazione fintech non è quindi sufficiente a tal fine.

D. Adeguamento della soglia per i depositi del pubblico da parte del Consiglio federale (cpv. 2)

Il Consiglio federale può adeguare l'importo di **CHF 100 milioni** tenendo conto della competitività e della capacità di innovazione della piazza finanziaria svizzera (art. 1b cpv. 2 LBCR). In casi singoli motivati, anche la FINMA deve avere la possibilità di derogare al limite massimo di CHF 100 milioni (art. 1b cpv. 5 LBCR). 38

In questo contesto, nel 2022 il Consiglio federale ha annunciato che occorre verificare se mantenere il **limite** di 100 milioni di CHF per l'accettazione di fondi della clientela. Anche se la FINMA, ai sensi dell'art. 1b cpv. 5 della LBCR, la limitazione crea incertezze su come la FINMA deciderà in ultima istanza. I criteri utilizzati dalla FINMA per concedere una deroga in singoli casi non sono stati finora resi pubblici. Anche il Consiglio federale non si è finora espresso in modo più concreto su un possibile adeguamento della soglia per i depositi del pubblico nell'ambito dell'art. 1b cpv. 2 LBCR. Resta quindi da attendere un primo caso di applicazione della norma speciale. 39

IV. PRESUPPOSTI PER L'AUTORIZZAZIONE (CPV. 3 E 4)

A. Oggetto sociale (cpv. 3 lett. a)

1. Considerazioni generali

Lo statuto o il **regolamento organizzativo e operativo** (ROO) devono descrivere con precisione, dal punto di vista oggettivo e territoriale, l'**ambito di attività** (art. 1b cpv. 3 lett. a LBCR; art. 14b cpv. 1 OB). L'ambito di attività e la sua estensione geografica devono corrispondere alle possibilità finanziarie e all'organizzazione amministrativa della richiedente (art. 14b cpv. 2 OB). Agli istituti fintech è vietato investire o remunerare i depositi del pubblico o gli attivi basati su criptovalute da essi raccolti (art. 1b cpv. 1 lett. b LBCR). Non è possibile inserire «a titolo precauzionale» attività negli statuti o nel regolamento interno (OGR). 40

Gli statuti o il regolamento interno (OGR) devono rispecchiare in modo dettagliato («preciso») l'**attività attuale** di una persona ai sensi dell'art. 1b della LBCR, sotto il profilo oggettivo, territoriale e personale. Le attività future dipendono di norma dall'esperienza maturata in altre attività e devono 41

pertanto essere concretizzate al momento della richiesta di autorizzazione ed essere preventivamente approvate dalla FINMA (cfr. art. 8 cpv. 2 OB). In tal senso, nell'ambito della procedura di autorizzazione viene spesso richiesta una concretizzazione delle relative disposizioni negli statuti e nel regolamento interno.

42 La domanda di autorizzazione deve contenere le seguenti **informazioni generali**:

- motivi e finalità per l'ottenimento di un'autorizzazione in qualità di persona ai sensi dell'art. 1b della LBCR;
- descrizione dettagliata dell'attività e dell'organizzazione previste, compreso l'ambito di attività previsto dal punto di vista oggettivo e geografico, nonché la tipologia di clientela a cui ci si rivolge;
- estratto del registro di commercio;
- estratto del registro delle esecuzioni (non più vecchio di 3 mesi) della richiedente;
- dichiarazione relativa ai procedimenti pendenti e conclusi (modulo B1; firmato e datato) della richiedente;
- informazioni sulle società del gruppo, nonché sulle partecipazioni e/o su altre presenze (filiali o rappresentanze) della richiedente.

43 Le informazioni richieste relative all'**attività commerciale, all'organizzazione e alla governance** della richiedente comprendono:

- descrizione dettagliata delle attività commerciali e dei relativi processi;
- piano aziendale comprensivo di bilancio preventivo (bilancio, conto economico) per i prossimi tre esercizi con scenari ottimistico, realistico e pessimistico;
- piano di liquidità per il primo esercizio secondo lo scenario pessimistico del piano aziendale (su base mensile);
- statuto, regolamento organizzativo e linee guida (regolamenti e direttive) adeguati all'attività commerciale di una persona ai sensi dell'art. 1b della LBCR;
- organigramma con l'indicazione dei dirigenti e gli ETP per unità organizzativa;

- Informazioni sui locali aziendali (compresa la presentazione del contratto di locazione), sull'infrastruttura e sul personale;
- Organizzazione e regolamenti o direttive relativi alla gestione dei rischi, alla compliance e al sistema di controllo interno (comprese le direttive ai sensi dell'LRD);
- Informazioni e documentazione relative all'esternalizzazione di attività (compresa l'analisi dei rischi, le linee guida relative a obiettivi, requisiti, competenze e processi, l'inventario delle funzioni esternalizzate e i contratti di esternalizzazione);
- Informazioni e documentazione relative alla gestione dei rischi operativi (in particolare i rischi legati alle tecnologie dell'informazione e della comunicazione (TIC), i rischi informatici, i rischi relativi ai dati critici, rischi derivanti dalla progettazione e dall'implementazione del Business Continuity Management (BCM) e, se del caso, rischi derivanti dall'attività transfrontaliera di prestazione di servizi), garanzia della resilienza operativa e relativa rendicontazione;
- Pianificazione ICT con dettagli sulla funzionalità tecnica e operativa delle singole applicazioni e sulla loro criticità;
- Panoramica del panorama ICT e applicativo previsto e delle interconnessioni interne dei sistemi (comprese le interfacce con sistemi di terzi, le linee guida relative ai sistemi ICT e alla sicurezza ICT, nonché relative all'archiviazione e alla sicurezza dei dati) all'avvio dell'attività operativa;
- Descrizione delle modalità di detenzione dei depositi del pubblico (separazione dai fondi propri dell'impresa) e delle modalità con cui viene garantito il rispetto della soglia di 100 milioni di CHF;
- se previsto: descrizione tecnica dettagliata delle modalità di custodia delle attività basate su criptovalute;
- indicazioni dettagliate sulle informazioni fornite ai clienti ai sensi dell'art. 7a OB, in particolare sui rischi e sull'assenza di una garanzia dei depositi.
- Descrizione di eventuali conflitti di interesse e relative misure volte a tutelare i clienti da eventuali pregiudizi ai sensi dell'art. 14g OB.

Gli istituti titolari di un'autorizzazione fintech possono in linea di principio 44
presentare i modelli di business più disparati (tra cui crowdfunding, traffico

dei pagamenti, sia mediante l'utilizzo di tecnologie tradizionali sia di applicazioni basate sulla tecnologia DLT/blockchain, ecc.) . Nella pratica, tuttavia, si è finora constatato che sono soprattutto i **fornitori di servizi di pagamento** a ricorrere a questa categoria di autorizzazione.

- 45 Oltre alle attività che comportano l'obbligo di autorizzazione in qualità di istituto fintech, quest'ultimo può in linea di principio fornire anche servizi accessori che, a loro volta, – se considerati isolatamente – non comporterebbero alcun obbligo di autorizzazione. La FINMA subordina la prestazione di tali servizi accessori, che di per sé non comporterebbero alcun obbligo di autorizzazione ma aumentano i rischi dell'istituto, all'attuazione di adeguate misure di mitigazione del rischio (cfr. art. 14e cpv. 1 OB). Qualora tali misure non vengano adottate o qualora le disposizioni relative agli istituti fintech non consentano misure adeguate di limitazione del rischio, la prestazione di un servizio accessorio non è compatibile con l'autorizzazione come istituto fintech.

2. Custodia di depositi del pubblico e di valori patrimoniali basati su criptovalute (cpv. 3 lett. a)

a. Custodia di depositi del pubblico

- 46 Gli istituti fintech devono custodire i depositi del pubblico (ai sensi dell'art. 5 OB) e gli attivi basati su criptovalute in custodia collettiva (ai sensi dell'art. 5a OB) **separatamente dai propri fondi** (art. 14f, cpv. 1, lett. a OB) . In tal caso è eventualmente possibile una revisione limitata ai sensi dell'art. 727a del Codice delle obbligazioni (CO) (art. 14f cpv. 1 lett. b OB *e contrario*) . Secondo un'interpretazione letterale dell'art. 14f cpv. 1 lett. a OB, non è consentito depositare fondi dei clienti su un conto di un fornitore di servizi terzo, ad esempio un gestore di pagamenti sprovvisto di autorizzazione bancaria. Eventuali depositi necessari presso tali gestori di pagamenti dovrebbero quindi essere prefinanziati con fondi dell'istituto fintech .
- 47 Una **deroga** a tale separazione è concessa qualora i depositi del pubblico possano essere contabilizzati in qualsiasi momento separatamente dai fondi propri e venga effettuata una revisione ordinaria ai sensi dell'art. 727 CO (art. 14f cpv. 1 lett. b OB).
- 48 Le imprese sono tuttavia tenute in primo luogo a trasferire i fondi raccolti secondo la destinazione prevista dall'accordo con i clienti o – qualora ciò non

sia lo scopo o non sia possibile – a rimborsarli ai clienti. Se un trasferimento immediato non è possibile o non è previsto in base all'**accordo con il cliente**, l'impresa può custodire i depositi. Tale «custodia» dei depositi non è vincolata ad alcun termine, ma è soggetta a determinate condizioni: i depositi devono essere sempre custoditi nell'interesse dei clienti e non possono essere né investiti né fruttati. Devono essere detenuti come depositi a vista presso una banca o sotto forma di attività altamente liquide.

Il **progetto di consultazione** del 21 giugno 2018 non conteneva ancora la 49
lett. b. La custodia separata dei depositi del pubblico raccolti è stata uno dei principali punti di critica durante la consultazione, poiché avrebbe comportato un notevole onere organizzativo e amministrativo per gli istituti FinTech. In risposta a tali critiche, il Consiglio federale ha previsto alla lett. b la «separazione contabile» a condizione che venga effettuata una revisione ordinaria ai sensi dell'art. 727 CO.

La detenzione dei depositi del pubblico ricevuti è soggetta al **divieto legale 50
di investimento e di remunerazione**. Ciò significa che essi devono essere detenuti in modo tale da che escluda in larga misura i rischi per i clienti. Devono inoltre essere disponibili in forma liquida, in modo da poter essere trasferiti o rimborsati secondo la destinazione entro un termine ragionevole. Una possibilità è rappresentata in particolare dal versamento dei fondi come depositi a vista su un conto bancario presso una banca o un altro soggetto ai sensi dell'art. 1b LBCR. In tal caso non dovrebbero sussistere restrizioni restrittive al prelievo.

In conformità con il principio di separazione ai sensi dell'art. 14^f cpv. 1 lett. a 51
dell'Ordinanza sulle banche (OB), i depositi del pubblico possono essere detenuti come **depositi a vista** presso una banca o un istituto fintech e/o come **High Quality Liquid Assets (HQLA)** di categoria 1 ai sensi dell'art. 15a dell'Ordinanza sulla liquidità del 30 novembre 2012 (LiqV) (art. 14^f cpv. 2 OB). I depositi del pubblico possono quindi essere detenuti sotto forma di monete, banconote o averi presso la banca centrale, oppure essere investiti in determinati titoli negoziabili emessi da debitori specifici (come ad esempio i governi centrali), senza violare il divieto di investimento. Gli istituti di moneta elettronica non sono in linea di principio riconosciuti in questo contesto, a meno che non sussista una garanzia dei depositi o una garanzia analoga per i fondi raccolti.

- 52 I depositi del pubblico devono essere sempre detenuti nella valuta del **diritto al rimborso** (art. 14^f cpv. 3 OB). Ciò significa in particolare che i depositi del pubblico in attività basate su criptovalute detenute in custodia collettiva devono essere mantenuti in tale forma (art. 14^f cpv. 4 OB). La possibilità di detenere i depositi del pubblico in HQLA consente agli istituti, se del caso, di evitare tassi d'interesse negativi. Tuttavia, ciò comporta determinati rischi d'investimento per i clienti, il che può comportare requisiti più elevati in materia di capitale minimo.
- 53 I clienti non dovrebbero, per quanto possibile, essere esposti a rischi aggiuntivi, in particolare **rischi di cambio**. Per questo motivo, i depositi del pubblico raccolti devono essere detenuti esclusivamente nella valuta in cui sussiste un eventuale diritto di restituzione.
- 54 Le disposizioni relative ai **depositi privilegiati** (art. 37a LBCR) e al pagamento immediato (art. 37b LBCR) **non si applicano ai depositi presso istituti fintech** (art. 1b cpv. 4 lett. d LBCR), poiché, secondo l'attuale interpretazione del legislatore, sarebbero sproporzionate. Di conseguenza, gli istituti fintech sono esentati dall'obbligo di aderire all'autoregolamentazione in materia di garanzia dei depositi e dai requisiti di liquidità più elevati applicabili alla **garanzia dei depositi**.

b. Monitoraggio della soglia per i depositi del pubblico (cpv. 6)

- 55 Il **limite** di CHF 100 milioni per i depositi del pubblico e i token di pagamento custoditi in modo collettivo è obbligatorio (fatto salvo l'art. 1b cpv. 2 e 5 LBCR). Nella domanda di autorizzazione occorre descrivere in che modo viene verificato il rispetto della soglia di CHF 100 milioni di depositi del pubblico.
- 56 Gli istituti fintech devono pertanto disporre, per quanto riguarda il monitoraggio del valore soglia, di procedure documentate, controlli (responsabilità, periodicità), rendiconti (comprese le previsioni) e ulteriori misure. A tal fine può essere opportuno, ad esempio, un **sistema graduale di misure**, ad esempio a CHF 70, 80, 90 e 99 milioni. A partire da una certa soglia occorre prevedere, in linea di principio, limitazioni tecniche affinché non vengano più accettati nuovi depositi del pubblico e questi vengano restituiti. Inoltre, occorre regolamentare il coordinamento con la FINMA.

Se più istituti fintech costituiscono un **gruppo finanziario** ai sensi dell'art. 22 57 OB, la soglia di 100 milioni di CHF deve essere calcolata per l'intero gruppo (art. 24a cpv. 1 OB), a meno che le società del gruppo non siano manifestamente indipendenti l'una dall'altra. Ciò mira a impedire che questa categoria di autorizzazione venga utilizzata per l'arbitraggio regolamentare nel settore della raccolta di depositi del pubblico. Si tratta quindi di impedire la creazione di strutture volte ad aggirare la soglia di CHF 100 milioni.

3. Custodia degli attivi basati su criptovalute

Gli **attivi basati su criptovalute** in custodia collettiva devono essere 58 detenuti in Svizzera e nella forma in cui sono stati accettati (art. 14f, cpv. 4, OB). Il potere di disposizione sulle chiavi private spetta quindi, in linea di principio, obbligatoriamente ed esclusivamente agli istituti fintech o alle banche domiciliati in Svizzera. Gli istituti fintech definiscono nelle direttive interne le modalità di gestione delle chiavi crittografiche che consentono l'accesso agli attivi basati su criptovalute. Le direttive interne devono, tra l'altro, a. disciplinare la gestione e il controllo di tutte le chiavi necessarie, ovvero la conservazione sicura, la messa a disposizione, la trasmissione sicura e il ritiro delle chiavi crittografiche non valide o compromesse.

Le **chiavi crittografiche** possono, ad esempio, essere memorizzate in un 59 modulo di sicurezza hardware (HSM). Per quanto riguarda la sicurezza degli HSM, l'istituto fintech dovrebbe orientarsi allo standard FIPS (FIPS) 140 del governo degli Stati Uniti. Lo standard definisce i requisiti minimi di sicurezza per i moduli crittografici nei prodotti informatici ed è sancito nella sezione 5131 dell'Information Technology Management Reform Act del 1996.

In linea di principio, occorre garantire che l'accesso agli asset basati sulla 60 crittografia sia possibile solo tramite **procedura di firma multipla**. Una delle chiavi parziali deve essere gestita da un membro della direzione. L'utilizzo di una chiave privata deve essere obbligatoriamente preceduto dall'identificazione dell'avente diritto. Per le transazioni a partire da un determinato importo è necessario ottenere l'approvazione di un secondo membro della direzione. Per la firma di transazioni di importo esiguo è possibile prevedere una procedura semplificata di gestione delle chiavi. L'utilizzo di chiavi private per la firma delle transazioni è soggetto a norme di documentazione, il cui rispetto deve essere verificato regolarmente nell'ambito del sistema di controllo interno (SCI).

- 61 Gli istituti fintech devono inoltre garantire che, in caso di smarrimento di chiavi parziali (ad es. a causa di un incendio o simili), sia possibile accedere alle attività basate su criptovalute tramite una **chiave di backup/ripristino/master** (*seed*). Tale chiave deve essere conservata in un luogo separato dalle altre chiavi private (ad es. in una cassaforte presso un fornitore di servizi finanziari) . L'accesso e lo scambio devono essere disciplinati in una direttiva interna.
- 62 La FINMA può fissare, in singoli casi, un **limite massimo** per gli asset basati su criptovalute, qualora ciò appaia opportuno alla luce dei rischi connessi all'operazione. A tal fine, l'autorità di vigilanza tiene conto in particolare della funzione degli asset basati su criptovalute, delle tecnologie sottostanti e dei fattori di riduzione del rischio (art. 4^{sexies} LBCR).
- 63 Gli istituti che offrono servizi di custodia di asset basati su criptovalute devono redigere un *Digital Asset Resolution Package* (DARP). Lo scopo di questo documento è garantire che, in caso di fallimento dell'istituto, un liquidatore esterno possa liquidare rapidamente gli asset basati su criptovalute a favore dei clienti, in modo da ridurre al minimo l'onere e i costi per una restituzione regolare. A tal fine, il DARP deve contenere le informazioni più importanti per l'identificazione e la tempestiva messa in sicurezza degli asset basati su criptovalute, come ad esempio i dati relativi a tutte le persone necessarie per la custodia e le trans degli asset basati su criptovalute, comprese le relative istruzioni, indicazioni per l'accesso a una copia aggiornata del registro interno (Internal Ledger), comprese le relative istruzioni, indicazioni su eventuali depositari terzi, compresi i dati di contatto delle persone responsabili per conto della banca presso il depositario terzo, ecc. È necessario garantire che l'istituto aggiorni regolarmente il DARP.

B. Organizzazione amministrativa adeguata (cpv. 3 lett. a)

- 64 Gli istituti fintech devono disporre di un'**organizzazione amministrativa** adeguata alla loro attività commerciale (ambito di attività e relativa estensione territoriale) (art. 1b cpv. 3 lett. a LBCR; art. 14b cpv. 2 OB).

1. Forma giuridica, sede e luogo di attività

- 65 Gli istituti fintech assumono la **forma giuridica** di una società per azioni, di una società in accomandita per azioni o di una società a responsabilità limitata

e hanno sede in Svizzera (art. 14a OB). Ciò al fine di garantire una vigilanza adeguata.

Dal punto di vista dogmatico, il rinvio generale per analogia di cui all'art. 1b 66 cpv. 1 LBCR può essere interpretato nel senso che la **cooperativa**, contrariamente a quanto previsto dal testo dell'ordinanza, dovrebbe essere riconosciuta come forma giuridica ammissibile. Tuttavia, a causa delle difficoltà legate al capitale sociale che deve essere mantenuto in modo permanente, alle rigide regole organizzative e decisionali (in particolare il diritto di voto per testa) e delle quote sociali, che non possono essere cartolarizzate come titoli, tale forma giuridica non è tuttavia adeguata per la gestione di un istituto fintech.

L'attività principale, ovvero la gestione effettiva, deve essere esercitata in 67 **Svizzera** e l'istituto fintech deve essere effettivamente diretto dalla Svizzera. Le persone incaricate della gestione devono avere il domicilio in un luogo dal quale possano effettivamente esercitare la gestione (art. 14a cpv. 2 e art. 14c OB).

Le persone incaricate della **gestione** devono avere il proprio domicilio nelle 68 vicinanze della sede della richiedente. È richiesto che il domicilio sia stabilito nelle vicinanze o in Svizzera. Secondo l'attuale prassi della FINMA, ci si aspetta che in ogni giorno lavorativo almeno una parte delle persone incaricate della gestione sia presente presso la sede. Ciò ha lo scopo di garantire che un istituto fintech svizzero non sia di fatto gestito dall'estero.

Secondo l'attuale prassi di vigilanza, nel caso di garanti titolari di un permesso 69 di soggiorno di breve durata a tempo determinato (permesso L) il rischio di estinzione dei **diritti di soggiorno** deve essere affrontato in modo adeguato. L'istituto deve tenere conto di tale rischio nell'ambito della propria gestione dei rischi e proteggerne le conseguenze mediante misure adeguate, in particolare procedure di segnalazione, di sostituzione e di successione.

Per quanto riguarda la **ragione sociale**, l'art. 1 cpv. 4 LBCR stabilisce che i 70 termini «banca» o «banchiere», da soli o in combinazioni di parole nella ragione sociale, nella designazione dell'oggetto sociale e nella pubblicità commerciale, a tutela dei creditori, possa essere utilizzata solo per gli istituti che dispongono di un'autorizzazione della FINMA come banca; sono inclusi in questo ambito i termini analoghi in tutte le lingue nazionali e in tutte le lingue straniere, nonché, in linea di principio, anche le combinazioni di parole

che alludono a un'attività bancaria, sono inclusi. Le combinazioni di parole contenenti gli elementi «*bank*» o «*banking*» sono quindi da considerare con cautela (anche sul sito web, nel registro delle imprese o negli statuti). Ciò comprende anche varianti più creative come «*non-bank*» o «*neo-bank*». Non dovrebbero invece presentare problemi termini quali «*money accounts*», «*payment accounts*», «*payments services*» o combinazioni simili, poiché i servizi di pagamento non devono necessariamente essere forniti da una banca, ma può essere sufficiente anche l'affiliazione a un OAD.

- 71 In base a un'applicazione per analogia dell'art. 4^{quater} LBCR agli istituti fintech, questi ultimi devono quindi astenersi, sia in Svizzera che all'estero, da qualsiasi **pubblicità** ingannevole o invadente che faccia riferimento alla loro sede svizzera o alle disposizioni svizzere a tutela dei creditori.

2. Organi

- 72 Se l'oggetto sociale o l'entità dell'attività di un istituto fintech richiede un organo specifico per la direzione generale, la vigilanza e il controllo, tale organo deve essere composto da almeno tre membri (art. 14d cpv. 1 OB). Gli istituti fintech devono di norma disporre di **organi di amministrazione e di direzione**, per cui l'organo preposto alla direzione generale, alla vigilanza e al controllo (consiglio di amministrazione) deve comprendere almeno tre membri. Almeno un terzo dei membri del consiglio di amministrazione deve essere indipendente dalla direzione (art. 14d cpv. 2 OB).
- 73 Un membro dell'organo di direzione generale è considerato **indipendente** se:
- non è impiegato presso l'istituto in altra funzione e non lo è stato nemmeno negli ultimi 2 anni;
 - negli ultimi 2 anni non è stato impiegato presso la società di revisione dell'istituto in qualità di revisore responsabile per l'istituto;
 - non intrattiene con l'istituto alcun rapporto d'affari che, per la sua natura o portata, possa dar luogo a un conflitto di interessi;
 - non sia una persona qualificata (ai sensi dell'art. 3 cpv. 2 lett. c^{bis} LBCR) dell'istituto né ne rappresenti una; e
 - in linea di principio non abbia alcun rapporto di vicinanza (parentela, matrimonio o convivenza) con un membro della direzione.

La FINMA può concedere, in casi motivati, **deroghe** ai requisiti relativi agli organi (art. 14d cpv. 4 OB). La separazione dei poteri e delle funzioni non è quindi assoluta. La FINMA può ad esempio consentire che un istituto fintech disponga solo di una direzione, ma non di un consiglio di amministrazione. Tale deroga è destinata a istituti di dimensioni molto ridotte in fase di avvio. In particolare, è ipotizzabile che alle *start-up* vengano concesse deroghe temporanee ai requisiti relativi all'organizzazione amministrativa fino al raggiungimento di determinati obiettivi di crescita; ad esempio, solo a partire da un ricavo lordo di CHF 1 milione siano previsti membri indipendenti del consiglio di amministrazione (e, a partire da CHF 1,5 milioni, funzioni di controllo indipendenti). 74

Il concetto di organo si riferisce alle **persone fisiche**. Le persone giuridiche non sono quindi considerate organi. La FINMA verifica, per i membri del consiglio di amministrazione e della direzione, la cosiddetta **garanzia di un'attività impeccabile**. Tale verifica è per sua natura personale e presuppone la valutazione dell'integrità, della reputazione personale, delle qualifiche professionali, dell'esperienza e dei conflitti di interesse. 75

La **documentazione** richiesta relativa agli organi comprende: 76

- la composizione dell'organo incaricato dell'amministrazione, con l'indicazione del presidente, del vicepresidente e dei membri di eventuali comitati; nonché
- indicazioni sulla composizione, l'organizzazione e le competenze della direzione.

3. Infrastruttura e personale

a. Locali commerciali

La richiedente deve disporre di **locali commerciali idonei**. Per quanto riguarda le dimensioni, possono essere sufficienti un ufficio e una sala riunioni. Qualora non si disponga di un immobile di proprietà, è necessario presentare un contratto di (sub)locazione. Sono necessarie informazioni sulle possibilità/restrizioni di accesso, sulla possibilità di chiudere a chiave i locali e gli arredi, nonché sullo svolgimento delle attività quotidiane nel rispetto del segreto informatico e bancario (ad es. un accordo di riservatezza che garantisca il rispetto delle norme di riservatezza applicabili alla richiedente 77

nell'attività quotidiana [in particolare per quanto riguarda il traffico di persone, la corrispondenza postale e l'infrastruttura fisica delle TIC]). È inoltre necessario che la gestione operativa effettiva della società avvenga dai locali commerciali in questione.

b. Risorse umane

- 78 Per quanto riguarda le risorse umane, è di fondamentale importanza che l'istituto fintech abbia coperto i posti di lavoro necessari e sia in grado di reagire rapidamente qualora fosse necessario **personale** aggiuntivo per l'attività aziendale. A tal fine occorre fornire le informazioni del caso e illustrare, idealmente tramite un grafico, gli equivalenti a tempo pieno (FTE) occupati, compresi i settori di attività.

c. Infrastruttura tecnica

- 79 Gli istituti fintech di norma non dispongono di una propria infrastruttura ICT fisica, ad eccezione dei terminali e delle infrastrutture di allacciamento elettrico, telefonico e Internet. La maggior parte dell'**infrastruttura ICT** è spesso basata sul cloud, il che comporta solitamente dei rischi.
- 80 Nell'ambito della domanda è necessaria una descrizione più dettagliata dell'architettura ICT prevista e dei componenti ICT necessari per le attività pianificate. Di conseguenza, è richiesta anche una pianificazione ICT con indicazioni sulla **operatività** tecnica e operativa delle singole applicazioni e sulla loro criticità. L'istituto fintech deve fornire indicazioni in merito all'operatività operativa e tecnica delle proprie applicazioni ICT. In un calendario deve illustrare lo stato di avanzamento e l'implementazione delle applicazioni da esso previste ed esprimersi sulla loro criticità in vista della messa in funzione.

4. Esternalizzazioni

a. Esternalizzabilità

- 81 Gli istituti fintech possono in linea di principio esternalizzare funzioni e attività (principio di esternalizzabilità). L'**esternalizzazione** di funzioni essenziali è quindi consentita. I requisiti della circolare FINMA 2018/3 «Outsourcing» si applicano agli istituti fintech in misura adeguata. I requisiti

devono essere attuati tenendo conto delle dimensioni, della complessità, della struttura e del profilo di rischio dell'istituto.

Per garantire la visione d'insieme e il controllo, le funzioni essenziali 82
esternalizzate e i relativi fornitori di servizi devono essere riportati nell'**OGR**.

Le imprese delle categorie di vigilanza da 1 a 3 dispongono di una funzione 83
autonoma di controllo dei rischi e di compliance in qualità di organi di controllo indipendenti. Per gli **istituti fintech** è sufficiente che nella direzione sia designata una persona responsabile di tali funzioni. I compiti operativi di gestione dei rischi e di compliance sono esternalizzabili in tutte le categorie di vigilanza.

Non sono esternalizzabili la direzione generale, la vigilanza e il controllo da 84
parte del consiglio di amministrazione, i compiti dirigenziali centrali della direzione aziendale nonché le funzioni che comportano decisioni strategiche. Ciò vale anche per le decisioni relative all'avvio e alla cessazione dei rapporti d'affari.

b. Rilevanza

La qualificazione come esternalizzazione rilevante o irrilevante può sollevare 85
interrogativi. Inoltre, occorre distinguere le esternalizzazioni dalle collaborazioni con fornitori di servizi terzi, che forniscono servizi che non fanno parte dell'attività commerciale o delle funzioni operative dell'istituto fintech nei confronti dei propri clienti, ad esempio rapporti d'affari diretti con l'istituto fintech o con i clienti dello stesso. In quest'ultimo caso, l'istituto fintech non agisce in qualità di parte contraente, bensì di intermediario. La **rilevanza** va di norma ritenuta affermativa, qualora il fornitore di servizi abbia accesso a dati critici del soggetto sottoposto a vigilanza e possa estrarre o addirittura manipolare tali dati. A favore della rilevanza di un'esternalizzazione depone anche il fatto che un'interruzione del servizio da parte del fornitore di servizi comprometta direttamente l'attività operativa del soggetto sottoposto a vigilanza. In linea di tendenza, sempre più funzioni devono essere classificate come essenziali a causa della loro dipendenza operativa diretta.

86 Di norma, nell'ambito dell'attività degli istituti fintech, si presume che si tratti di un **esternalizzazione essenziale** per i seguenti servizi e funzioni:

- servizi software e di server che vanno oltre il semplice supporto, nella misura in cui influenzano direttamente l'attività operativa;
- sistema bancario centrale (purché sussista una dipendenza diretta e critica in termini di tempo);
- infrastruttura IT basata su cloud;
- soluzioni SaaS, qualora la gestione avvenga presso il fornitore di servizi e sussista quindi una dipendenza diretta per l'attività operativa);
- gateway SIC;
- sponsor BIN/SIC (a differenza degli emittenti di carte);
- fornitori di transazioni in valuta estera, qualora l'integrazione dei servizi vada ben oltre il tradizionale rapporto di corrispondenza bancaria;
- fornitori di servizi di cambio valuta, qualora il processo sia critico per l'erogazione del servizio da parte dell'istituto fintech;
- tutte le funzioni/istanze di controllo: controllo dei rischi, funzione di compliance, unità specializzata in materia di riciclaggio di denaro, revisione interna;
- sistemi KYC (identificazione e verifica in caso di accesso a dati critici);
- Identificazione a due fattori;
- Monitoraggio delle transazioni;
- Funzione di responsabile della protezione dei dati o consulente in materia.

87 **Non sono generalmente considerati essenziali** i seguenti servizi e funzioni esternalizzati:

- Servizi di verifica (di indirizzi di residenza o numeri di cellulare);
- fornitura di infrastrutture di base (ad es. Internet) e banche dati (ad es. elenchi delle sanzioni per il KYC);
- tipici servizi di supporto (quali consulenza legale, consulenza economica, contabilità, rendicontazione, consulenza fiscale, risorse umane, pubbliche relazioni e comunicazione, nonché marketing), poiché questi sono più facilmente sostituibili e in linea di principio non sussistono dipendenze.

c. Inventario

Gli istituti fintech devono tenere un **inventario** aggiornato delle funzioni 88 esternalizzate. Esso contiene una descrizione della funzione esternalizzata, indica i fornitori di servizi (compresi i subappaltatori) e i destinatari dei servizi, nonché l'organo responsabile all'interno dell'azienda.

d. Analisi dei rischi

Nell'ambito dell'esternalizzazione, la richiedente deve redigere un'**analisi dei 89 rischi** che comprenda le principali considerazioni economiche e operative, nonché i rischi e le opportunità ad esse connessi. Qualora più funzioni vengano esternalizzate allo stesso fornitore di servizi, occorre tenere conto del rischio di concentrazione.

e. Selezione, istruzione e controllo del fornitore di servizi

Nella **selezione** del fornitore di servizi occorre tenere conto e verificare la 90 sua idoneità tecnica, nonché le sue risorse finanziarie e di personale. Nel decidere in merito all'esternalizzazione e nella scelta del fornitore di servizi, occorre considerare anche le possibilità e le conseguenze di un eventuale cambio di fornitore. Il fornitore di servizi deve garantire la continuità della prestazione.

Nell'ambito delle **istruzioni**, le competenze dell'impresa e del fornitore di 91 servizi devono essere definite e delimitate contrattualmente, in particolare per quanto riguarda le interfacce e le responsabilità.

La funzione esternalizzata deve essere integrata nel **sistema di controllo 92 interno** (SCI) dell'impresa. I rischi significativi connessi all'esternalizzazione devono essere sistematicamente identificati, monitorati, quantificati e gestiti. All'interno dell'impresa deve essere designato un organo responsabile del monitoraggio e della gestione del fornitore di servizi. Le prestazioni del fornitore di servizi devono essere monitorate e valutate costantemente, affinché, se necessario, possano essere adottate tempestivamente le misure del caso.

f. Revisione e vigilanza

L'impresa, la sua società di revisione e la FINMA devono essere in grado di 93 verificare il rispetto delle disposizioni di vigilanza da parte del fornitore di

servizi. A loro favore deve essere concesso contrattualmente un **diritto di ispezione e di verifica** in qualsiasi momento, illimitato e senza ostacoli, in relazione alla funzione esternalizzata.

- 94 Le attività di verifica possono essere delegate all'organo di revisione del fornitore di servizi, a condizione che questo disponga della necessaria competenza tecnica. In caso di tale **delega**, la società di revisione dell'impresa può basarsi sui risultati della revisione effettuati dall'organo di revisione del fornitore di servizi.
- 95 L'esternalizzazione di una funzione non deve ostacolare la **vigilanza** da parte della FINMA, in particolare in caso di esternalizzazione all'estero.
- 96 Se il fornitore di servizi non è soggetto alla vigilanza della FINMA, questi deve impegnarsi contrattualmente nei confronti della richiedente a fornire alla FINMA tutte le **informazioni e documenti** relativi al settore di attività esternalizzato di cui essa ha bisogno per la propria attività di vigilanza. Qualora le attività di revisione siano delegate all'organo di revisione del fornitore di servizi, la relativa relazione deve essere messa a disposizione, su richiesta, della FINMA, dell'organo di revisione interno e della società di revisione dell'impresa che esternalizza.

g. Contratti di esternalizzazione

- 97 In linea con gli obiettivi perseguiti con l'esternalizzazione, i requisiti relativi alla prestazione dei servizi devono essere definiti e documentati prima della stipula del contratto. Ciò comprende un'**analisi dei rischi** che comprenda le principali considerazioni economiche e operative, nonché i rischi e le opportunità ad esse connessi.
- 98 Le **competenze** del richiedente e del fornitore di servizi devono essere definite e delimitate contrattualmente, in particolare per quanto riguarda le interfacce e le responsabilità.
- 99 Il richiedente deve farsi concedere contrattualmente dal fornitore di servizi i **diritti di istruzione e di controllo** necessari per la sorveglianza e il controllo del fornitore di servizi da parte del fornitore di servizi. In caso di esternalizzazioni rilevanti per la sicurezza (in particolare nel settore IT), l'impresa e il fornitore di servizi stabiliscono contrattualmente i requisiti di sicurezza. Il loro rispetto deve essere monitorato dall'istituto fintech.

Al fine di verificare il rispetto delle disposizioni di vigilanza da parte del
fornitore di servizi, deve essere concesso contrattualmente un **diritto di**
ispezione e verifica in qualsiasi momento, completo e senza ostacoli in
relazione alla funzione esternalizzata.

Se il fornitore di servizi (estero) non è soggetto alla vigilanza della FINMA,
esso deve impegnarsi contrattualmente nei confronti dell'impresa a mettere a
disposizione della FINMA tutte le **informazioni e i documenti** necessari
all'attività di vigilanza relativi all'area di attività esternalizzata.

L'esternalizzazione deve basarsi su un contratto **scritto** o su un contratto in
altra forma che consenta la prova testuale. Oltre all'identificazione delle parti
e alla descrizione delle funzioni, il contratto deve contenere almeno i
contenuti sanciti nella Circolare FINMA 2018/3.

L'istituto garantisce di essere informato tempestivamente del ricorso o del
cambio di subappaltatori che svolgono funzioni essenziali. Qualora vengano
coinvolti tali subappaltatori, è necessario imporre loro gli obblighi e le
garanzie del fornitore di servizi necessari per l'adempimento della Circolare
FINMA 2018/3. La possibilità di ricorrere a subappaltatori deve inoltre essere
disciplinata nel regolamento interno (OGR).

In generale, devono essere adottate disposizioni contrattuali per l'attuazione
dei **requisiti** della Circolare FINMA 2018/3.

L'istituto deve definire le procedure interne di autorizzazione per i **progetti**
di esternalizzazione nonché le competenze relative alla stipula dei relativi
contratti.

h. Rendicontazione

L'attuazione della necessaria vigilanza e del controllo del fornitore di servizi
può avvenire, nel caso degli istituti fintech avvenire, tramite una regolare
rendicontazione da parte di un organo di revisione indipendente, tenendo
conto della possibilità di delegare le attività di verifica all'organo di revisione
del fornitore di servizi. Tale rendicontazione deve consentire una valutazione
dei rischi significativi connessi all'esternalizzazione e delle attività di controllo
del fornitore di servizi.

i. Situazioni relative al gruppo

- 10 Per quanto riguarda i requisiti relativi alla selezione, all'istruzione e al
7 controllo del fornitore di servizi, nonché alle condizioni contrattuali, è possibile tenere conto dei legami all'interno del gruppo/**gruppo**, a condizione che sia dimostrabile l'assenza dei rischi tipicamente associati all'esternalizzazione o che determinati requisiti non siano rilevanti o siano disciplinati in modo diverso.

j. Responsabilità e sicurezza

- 10 L'istituto fintech rimane **responsabile** nei confronti della FINMA come se
8 svolgesse autonomamente la funzione esternalizzata. Deve garantire in ogni momento una corretta gestione aziendale.
- 10 In caso di esternalizzazioni rilevanti ai fini della sicurezza (in particolare nel
9 settore IT), l'istituto e il fornitore di servizi stabiliscono **requisiti di sicurezza** contrattuali. Il rispetto di tali requisiti deve essere monitorato dall'impresa.
- 11 In tale contesto, l'istituto e il fornitore di servizi elaborano un **dispositivo di**
0 **sicurezza** che consenta il proseguimento della funzione esternalizzata in caso di emergenza. Nell'istituzione e nell'applicazione del dispositivo di sicurezza, l'impresa applica lo stesso standard di diligenza che adotterebbe se svolgesse autonomamente la funzione esternalizzata.

k. Esternalizzazioni all'estero

- 11 Le esternalizzazioni all'**estero** sono ammesse a condizione che l'istituto possa
1 garantire espressamente che esso stesso, la sua società di revisione e la FINMA possano esercitare e far valere i propri diritti di accesso e di verifica. Deve inoltre essere garantita la possibilità di risanamento o di liquidazione dell'istituto in Svizzera. L'accesso alle informazioni necessarie a tal fine deve infine essere possibile in qualsiasi momento in Svizzera.

l. Obblighi e deroghe

- 11 La FINMA può, in casi motivati, imporre **obblighi** all'istituto fintech oppure
2 esonerarlo, in tutto o in parte, dal rispetto della Circolare FINMA 2018/3.

Gli istituti valutano e decidono in merito alla rilevanza e all'attuazione delle disposizioni relative alla selezione del fornitore di servizi nell'ambito della loro **analisi dei rischi**. 11 3

Gli istituti fintech sono esentati dal requisito di una reintegrazione ordinata per quanto riguarda la reintegrazione della funzione esternalizzata. L'integrazione della funzione esternalizzata nel sistema di controllo interno può avvenire, nel caso degli istituti fintech, tramite una regolare **rendicontazione** da parte di un organo di revisione indipendente. Tale rendicontazione deve consentire una valutazione dei rischi significativi connessi all'esternalizzazione e delle attività di controllo del fornitore di servizi. 11 4

C. Corporate Governance: gestione dei rischi, controlli interni e compliance (cpv. 3 lett. b)

1. Principi fondamentali

Gli istituti fintech devono disporre di un sistema di **gestione dei rischi** adeguatamente dotato e di un **sistema di controllo interno (SCI) efficace**, che garantisca in particolare il rispetto delle disposizioni legali e interne all'azienda (**compliance**) (art. 1b cpv. 3 lett. b LBCR e art. 14e cpv. 1 OB). 11 5

La **gestione dei rischi** comprende le strutture organizzative, nonché i metodi e i processi finalizzati alla definizione delle strategie di rischio e delle misure di controllo dei rischi, nonché all'identificazione, all'analisi, alla valutazione, alla gestione, monitoraggio e rendicontazione dei rischi. 11 6

Il **sistema di controllo interno (SCI)** comprende l'insieme delle strutture e dei processi di controllo che, a tutti i livelli dell'istituto, costituiscono la base per il raggiungimento degli obiettivi di politica aziendale e per il corretto funzionamento dell'istituto. A tal fine, lo SCI comprende non solo attività di controllo a posteriori, ma anche attività di pianificazione e gestione. L'ICS si concentra sul raggiungimento degli obiettivi aziendali, sulla tutela del patrimonio aziendale, sulla garanzia di processi sicuri e sulla prevenzione o individuazione di irregolarità. Un ICS efficace comprende, tra l'altro, attività di controllo integrate nei flussi di lavoro, adeguati processi di gestione dei rischi e di compliance, nonché organi di controllo adeguati alle dimensioni, 11 7

complessità e al profilo di rischio dell'istituto, in particolare una funzione indipendente di controllo dei rischi e di compliance.

- 11 Tra gli esempi di potenziali rischi figurano malfunzionamenti interni delle
8 TIC, difficoltà legate a funzioni esterne, pandemie, la perdita di personale essenziale o di clienti chiave, carenze di liquidità, rischi legali, attacchi informatici, guasti ai sistemi, interruzioni delle catene di approvvigionamento, interruzioni di corrente su vasta scala o prolungate, catastrofi naturali, perdita di dati, dipendenze da fornitori di servizi terzi, danni alla reputazione, nuove disposizioni normative, rischi di riciclaggio di denaro, terrorismo, frodi, ritardi nell'infrastruttura di pagamento o rischi valutari.
- 11 Per **compliance** si intende il rispetto delle disposizioni legali, regolamentari e
9 interne, nonché l'osservanza degli standard di mercato e delle norme deontologiche.
- 12 Gli istituti fintech devono pertanto garantire un'efficace identificazione,
0 valutazione, gestione e monitoraggio dei rischi connessi alla loro attività, nonché un efficace sistema di controllo interno (art. 14^e cpv. 1 OB) . Nella **documentazione interna e nelle direttive** deve essere specificato in che modo vengono soddisfatti i requisiti citati (art. 14^e cpv. 2 OB).
- 12 Il **segreto bancario** si applica anche agli organi, ai collaboratori, ai mandatar
1 o ai liquidatori degli istituti fintech (art. 47 cpv. 1 lett. a LBCR).
- 12 La Circolare FINMA 2017/1 «Corporate Governance – Banche» **non si**
2 **applica**, com'è opportuno, agli istituti fintech, poiché ciò non sarebbe utile alla luce del principio di proporzionalità ivi sancito. Per quanto riguarda la corporate governance, si applicano quindi le disposizioni della LBCR, dell'OBC e del CO (nonché, a titolo di autoregolamentazione, lo «Swiss Code of Best Practice for Corporate Governance»). La Circolare FINMA 2017/1 può tuttavia essere utilizzata come ausilio interpretativo per quanto riguarda la terminologia.
- 12 La **Circolare FINMA 2023/01** «Rischi operativi e resilienza – Banche» si
3 applica invece direttamente agli istituti fintech, sebbene alcune disposizioni non siano applicabili a tali istituti.

2. Funzioni di controllo indipendenti

Gli organi incaricati della **vigilanza** sulla compliance e sulla gestione dei rischi devono essere internamente indipendenti dall'attività a scopo di lucro (art. 14e cpv. 3 OB). La FINMA può concedere, in singoli casi, deroghe a tali requisiti se l'istituto fintech: a) realizza un ricavo lordo inferiore a CHF 1,5 milioni; oppure b) dimostri di disporre di un modello di business a basso rischio (art. 14e cpv. 5 OB).

L'istituto fintech può avvalersi di **terzi** per la vigilanza sulla compliance e la gestione dei rischi, a condizione che questi dispongano delle competenze, delle conoscenze e dell'esperienza necessarie per tale attività, nonché delle eventuali autorizzazioni richieste. Esso istruisce e sorveglia con cura i terzi coinvolti (art. 14e cpv. 4 OB).

Gli istituti fintech implementano di norma due livelli di controllo interno o **linee di difesa**: al primo livello, le unità operative orientate al risultato si fanno carico della gestione dei rischi, in particolare attraverso la loro diretta sorveglianza, controllo e rendicontazione, e garantiscono il rispetto dei requisiti legali nell'attività quotidiana (*first line of defense*). Al secondo livello (*second line of defense*), le funzioni di controllo dei rischi e di compliance sorvegliano i rischi e il rispetto delle disposizioni legali, regolamentari e interne. Al terzo livello, infine, può eventualmente avvenire la verifica da parte di una revisione interna (*third line of defense*). Se e in che misura un istituto fintech debba garantire questi tre livelli dipende essenzialmente dal caso concreto.

Di norma, con il controllo dei rischi e la funzione di compliance è richiesta solo una **seconda linea di difesa**. Gli organi responsabili del controllo dei rischi e della compliance devono essere indipendenti dall'attività orientata al profitto. L'applicabilità della deroga di cui all'art. 14e cpv. 4 OB deve essere valutata caso per caso. Nella valutazione del singolo caso occorre prestare particolare attenzione al rischio di conflitti di interesse. Se non è possibile escludere conflitti di interesse, deve essere prevista in ogni caso una funzione indipendente di gestione dei rischi e di compliance. Occorre inoltre tenere conto delle competenze e delle conoscenze delle persone coinvolte, nonché di un'eventuale attività commerciale già in essere.

La LBCR e, in particolare, l'art. 14e OB non menzionano la revisione interna per gli istituti fintech come strumento (presumibilmente obbligatorio) del

sistema di controllo interno. Una **revisione interna** non è quindi obbligatoria per gli istituti fintech. La necessità di disporre di tale funzione dipende, in base a considerazioni di rischio, essenzialmente dal singolo caso concreto, ovvero dalle dimensioni, dall'attività commerciale e dall'organizzazione esistente. Di norma è possibile rinunciare a una revisione interna.

3. Gestione dei rischi

a. Competenze

- 12 La gestione dei **rischi operativi** fa parte del sistema di gestione dei rischi a
9 livello di istituto. La politica di rischio e le linee guida della gestione dei rischi disciplinano la gestione dei rischi significativi, la tolleranza al rischio e i limiti di rischio che ne derivano in tutte le principali categorie di rischio.
- 13 L'**organo di alta direzione** approva le linee guida per la gestione dei rischi
0 operativi rilevanti per l'istituto e ne vigila sul rispetto. Approva almeno una volta all'anno la tolleranza al rischio per i rischi operativi in conformità con la politica di rischio e tenendo conto degli obiettivi strategici e finanziari dell'istituto. A tal fine tiene conto dei risultati delle valutazioni dei rischi e dei controlli. Accetta il livello di esposizione dell'istituto ai rischi operativi oppure decide in merito a un adeguamento della tolleranza al rischio e alle modifiche strategiche necessarie a tal fine, come ad esempio una modifica del modello di business.
- 13 In questo contesto, l'organo di alta direzione approva regolarmente **strategie**
1 documentate per la gestione delle TIC, dei rischi informatici, dei dati critici e del BCM, e ne vigila il rispetto.
- 13 La **direzione** garantisce in modo trasparente che i rischi operativi siano
2 identificati, valutati, limitati e monitorati e che sia l'impostazione che l'attuazione di tale gestione dei rischi operativi siano regolarmente verificate in termini di efficacia. Per limitare i rischi intrinseci ritenuti significativi (i cosiddetti «rischi principali» o «rischi chiave»), adotta, a seconda della situazione, misure supplementari o rafforzative specifiche per ciascun rischio.
- 13 Se necessario, la **FINMA** definisce, nell'ambito della vigilanza corrente su
3 tematiche specifiche, requisiti più approfonditi in materia di gestione dei rischi operativi. Ciò avviene secondo il principio di proporzionalità.

b. Inventario

I rischi operativi devono essere classificati in modo uniforme a livello dell'istituto e registrati in un **inventario**. La classificazione può avvenire sulla base della categorizzazione dei tipi di evento utilizzata per il calcolo del requisito minimo di fondi propri per i rischi operativi oppure mediante una tassonomia interna. La classificazione deve essere applicata in modo coerente in tutti i settori dell'istituto e in tutte le componenti della gestione dei rischi operativi.

c. Identificazione

I **rischi operativi** comprendono in particolare i rischi ICT, i rischi informatici, i rischi connessi ai dati critici, i rischi derivanti dalla progettazione e dall'attuazione del BCM nonché, se del caso, i rischi derivanti dall'attività di prestazione di servizi transfrontalieri. Ai fini della definizione ci si può riferire alla definizione giuridica di cui all'art. 89 dell'Ordinanza sui fondi propri (OFP), secondo cui per rischi operativi si intende il pericolo di perdite derivanti dall'inadeguatezza o dal malfunzionamento di procedure interne, persone e sistemi o da eventi esterni. Sono inclusi i rischi legali, ma non i rischi strategici e i rischi di reputazione.

Nell'**identificazione** dei rischi operativi occorre tenere conto sia dei fattori interni che di quelli esterni. I rischi operativi identificati devono essere valutati in modo comprensibile sia dal punto di vista dei rischi intrinseci che da quello dei rischi residui. Tra i fattori interni figurano, ad esempio, le modifiche relative a prodotti, attività, processi e sistemi, nonché i risultati delle verifiche e le perdite interne derivanti da rischi operativi. Tra i fattori esterni figurano, ad esempio, eventi con conseguenti perdite rilevati presso altri istituti, cambiamenti nella situazione di sicurezza (ad es. dovuti a fattori ambientali, attacchi informatici o terrorismo) o modifiche dei requisiti normativi.

L'identificazione e la valutazione dei rischi operativi devono basarsi almeno sui **risultati delle verifiche** e su valutazioni dei rischi e dei controlli effettuate regolarmente. I risultati delle verifiche dovrebbero (se disponibili) comprendere i risultati della revisione interna e della società di revisione esterna, nonché i risultati delle verifiche effettuate, ad esempio, dai settori

aziendali e organizzativi, dal controllo dei rischi, dalla funzione di compliance o dalle autorità di vigilanza.

d. Tolleranza al rischio

- 13 La **tolleranza al rischio** per i rischi operativi tiene conto sia della tolleranza
8 relativa ai rischi operativi intrinseci sia di quella relativa ai rischi operativi residui e viene monitorata sulla base di indicatori di rischio o di controllo.
- 13 La tolleranza al rischio relativa ai **rischi intrinseci** tiene conto delle decisioni
9 strategiche relative al modello di business o operativo, ad esempio la tolleranza nei confronti dei rischi intrinseci connessi alla gestione di determinati segmenti di clientela o paesi, all'offerta di determinati prodotti, all'utilizzo di processi prevalentemente manuali, alla dipendenza da un'infrastruttura IT complessa o a determinate esternalizzazioni.

e. Formazione del personale

- 14 Devono essere attuate misure volte a **sensibilizzare** il personale alla
0 riduzione dei rischi operativi rilevanti, in particolare dei rischi ICT, dei rischi informatici, dei rischi connessi ai dati critici e dei rischi derivanti dalla definizione e dall'attuazione del BCM, tenendo conto dei compiti, delle competenze e delle responsabilità del personale.

f. Controllo

- 14 Per valutare le attuali **misure di controllo e di mitigazione**, occorre in
1 particolare effettuare e documentare una valutazione periodica dell'efficacia dei controlli chiave da parte di un organismo di revisione indipendente (i cosiddetti *Design Effectiveness* e *Operating Effectiveness Testing*). I controlli chiave sono quelle misure di controllo e le misure di mitigazione che riducono al minimo i rischi intrinseci giudicati significativi.
- 14 Inoltre, occorre verificare regolarmente la **separazione funzionale** dei
2 compiti, delle competenze e delle responsabilità al fine di garantire l'indipendenza ed evitare conflitti di interesse. Le valutazioni dei rischi e dei controlli devono tenere conto dei rischi intrinseci, dell'efficacia delle misure di controllo e di mitigazione esistenti e i rischi residui.
- 14 Prima di **modifiche significative** a prodotti, attività, processi e sistemi,
3 devono essere effettuate valutazioni ad hoc dei rischi e dei controlli, tenendo

conto dei rischi operativi relativi al processo di modifica e allo stato obiettivo. Se necessario, l'istituto deve adeguare la tolleranza al rischio e attuare misure di controllo e di mitigazione.

g. Rendicontazione

Il **controllo dei rischi** riferisce all'organo di alta direzione almeno una volta all'anno e alla direzione aziendale almeno una volta ogni sei mesi in merito ai rischi operativi al livello più alto della classificazione, al loro confronto con la tolleranza al rischio definita, nonché ai dettagli relativi alle perdite interne significative. 14 4

Per quanto riguarda i rischi ICT e informatici rilevanti, la **relazione** almeno annuale alla direzione contiene inoltre informazioni sull'evoluzione di tali rischi, sull'efficacia dei relativi controlli chiave e sugli eventi interni ed esterni significativi connessi a tali rischi. 14 5

h. Rischi ICT

a. Strategia e governance

La gestione dei **rischi ICT** deve tenere conto degli standard e delle prassi pertinenti riconosciuti a livello internazionale, nonché dell'influenza dei nuovi sviluppi tecnologici sui rischi ICT. 14 6

La **direzione** garantisce che siano implementate e documentate procedure, processi e controlli, nonché compiti, competenze e responsabilità sia per la gestione delle modifiche (il cosiddetto *change management*) sia per il funzionamento delle TIC (il cosiddetto *run, maintenance*). A tal fine devono essere messe a disposizione risorse qualificate e adeguate. 14 7

b. Gestione delle modifiche

Per tutte le fasi dello sviluppo o dell'approvvigionamento delle TIC, la **gestione delle modifiche** deve definire procedure, processi e controlli. In ciascuna di queste fasi, essa deve tenere conto dell'impatto della modifica sui rischi informatici – in particolare sui requisiti di riservatezza, integrità e disponibilità. 14 8

L'istituto fintech deve garantire una **separazione** tra l'ambiente di sviluppo o di test e l'ambiente di produzione delle TIC. Ciò comprende anche una chiara 14 9

attribuzione delle TIC e una regolamentazione delle relative autorizzazioni di accesso.

- 15 Nello sviluppo e nell'approvvigionamento delle TIC, i requisiti funzionali e
0 non funzionali devono essere chiaramente definiti, approvarli e testarli e convalidarli in base alla loro **criticità**.

c. Gestione delle TIC

- 15 Nell'ambito della gestione delle TIC, l'istituto fintech deve tenere uno o più
1 inventari dei componenti TIC. L'**inventario** comprende componenti hardware e software, nonché le ubicazioni dei dati critici, e tiene conto sia delle dipendenze all'interno dell'istituto sia delle interfacce con importanti fornitori di servizi esterni. L'inventario deve essere disponibile tempestivamente e deve essere regolarmente verificato e aggiornato per garantirne la completezza e la correttezza.
- 15 Inoltre, l'istituto deve disporre di procedure, processi e controlli che
2 garantiscano la riservatezza, l'integrità e la disponibilità dell'ambiente di produzione ICT, tenendo conto della rispettiva **tolleranza al rischio**.
- 15 In questo contesto, occorre garantire che, in caso di malfunzionamento o
3 interruzione significativa, sia possibile assicurare una transizione senza intoppi dal funzionamento delle TIC ai processi previsti dal *Business Continuity Plan* (BCP) e dal *Disaster Recovery Plan* (DCP). A tal fine, l'istituto implementa adeguati **processi di backup e ripristino**, che vengono regolarmente testati e convalidati.
- 15 Infine, l'istituto deve inoltre attuare procedure, processi e controlli che
4 garantiscano una gestione delle TIC basata sul rischio quando si avvicina la fine dell'esercizio o quando è stata superata la data prevista per la dismissione.

d. Gestione degli incidenti

- 15 L'istituto fintech dispone di procedure, processi e controlli per la gestione di
5 **incidenti ICT significativi**, compresi quelli derivanti da dipendenze da fornitori di servizi esterni significativi e dall'outsourcing all'interno del gruppo. A tal fine occorre tenere conto dell'intero ciclo di vita degli incidenti ICT significativi e definire compiti, competenze e responsabilità per la gestione di tali incidenti.

La gestione degli incidenti ICT significativi deve essere coordinata e integrata con i **processi BCM e DRP**. 15 6

Gli incidenti ICT che l'istituto classifica come perturbazioni significative dell'esecuzione dei propri processi critici e che rivestono importanza ai fini della vigilanza devono essere segnalati senza indugio alla **FINMA**. 15 7

i. Rischi informatici

L'istituto deve definire compiti, competenze e responsabilità chiari anche in relazione ai **rischi informatici**. A tal fine, deve coprire almeno i seguenti aspetti in conformità con gli standard e le prassi riconosciuti a livello internazionale, garantendone l'efficace attuazione attraverso procedure, processi e controlli, e garantirne il continuo sviluppo e miglioramento: 15 8

- identificazione del **potenziale di minaccia** specifico dell'istituto derivante da attacchi informatici e valutazione dei possibili effetti in caso di sfruttamento delle vulnerabilità relative alle componenti inventariate delle TIC e ai dati elettronici critici;
- protezione delle componenti ICT inventariate e dei dati elettronici critici dagli attacchi informatici mediante l'attuazione di adeguate **misure di protezione** (come ad esempio backup dei dati, piani di ripristino, formazione informatica dei collaboratori, partecipazione a programmi di bug bounty o verifiche di sicurezza del codice sorgente), in particolare per quanto riguarda la riservatezza, l'integrità e la disponibilità;
- registrazione e individuazione tempestive degli attacchi informatici sulla base di un processo di **monitoraggio** sistematico e continuo delle componenti ICT inventariate e dei dati critici elettronici;
- **B reazione** alle vulnerabilità e agli attacchi informatici identificati attraverso lo sviluppo e l'implementazione di processi adeguati, al fine di avviare tempestivamente misure di contenimento e risoluzione; e
- garanzia di un tempestivo **B ripristino** del regolare svolgimento delle attività aziendali a seguito di attacchi informatici mediante misure adeguate.

La richiedente deve indicare i controlli del sistema di controllo interno (SCI) rilevanti per i rischi di sicurezza informatica e presentare i relativi documenti giustificativi (procedure, processi e controlli per individuare, contenere ed 15 9

eliminare un simile attacco informatico) nell'ambito dell'**analisi dei rischi informatici**.

- 16 **I rischi informatici** rientrano tra i rischi operativi e non sono equiparabili ai
0 rischi ICT. I rischi informatici presentano fattori di influenza esterni più marcati, quali lo sfruttamento di vulnerabilità attraverso diversi vettori di attacco, ad esempio nel caso di attacchi ransomware o Distributed Denial of Service (DDoS), nonché le minacce interne. Gli istituti devono pertanto includere nella propria gestione dei rischi una definizione autonoma dei rischi informatici che rispecchi la natura del rischio.
- 16 La gestione dei rischi informatici deve garantire che un attacco informatico
1 riuscito o parzialmente riuscito venga analizzato in relazione alla sua rilevanza per le componenti ICT critiche inventariate, i dati elettronici critici e i processi critici (compresi i servizi e le funzioni esternalizzati) e che venga rispettato l'**obbligo di segnalazione** alla FINMA. È importante che l'impresa fintech, in caso di eventuali servizi ICT esternalizzati, venga immediatamente informata in merito ad attacchi informatici riusciti o parzialmente riusciti e possa agire di conseguenza, e non solo per adempiere tempestivamente all'obbligo di segnalazione nei confronti della FINMA.
- 16 Una volta effettuata la valutazione iniziale della criticità e fornita
2 un'informativa preliminare informale al Key Account Manager competente della **FINMA** entro 24 ore, la segnalazione deve essere trasmessa secondo il catalogo dei requisiti della piattaforma di rilevamento EHP (campi obbligatori) entro 72 ore. Una volta conclusa la gestione del caso da parte dell'istituto, occorre presentare all'ufficio competente della FINMA un rapporto conclusivo sulle cause, commisurato al grado di gravità. In tale contesto, la richiedente deve illustrare in che modo garantisce il rispetto dell'obbligo di segnalazione di incidenti informatici riusciti o parzialmente riusciti di entità media, elevata o grave, venga rispettato.
- 16 La direzione fa eseguire regolarmente **analisi di vulnerabilità** (analisi volte a
3 identificare le vulnerabilità del software esistenti e le falle di sicurezza nell'infrastruttura IT) e **test di penetrazione** (verifica mirata e sfruttamento delle vulnerabilità del software e delle falle di sicurezza nell'ICT). Questi devono essere eseguiti da personale qualificato con risorse adeguate. A tal fine devono essere presi in considerazione tutti i componenti dell'ICT inventariati che sono accessibili tramite Internet. Inoltre, devono essere considerati i

componenti dell'ICT inventariati che non sono accessibili tramite Internet, ma che sono necessari per l'esecuzione di processi critici o che contengono dati critici in formato elettronico. La periodicità delle relative analisi e dei test deve essere stabilita nella documentazione corrispondente.

Sulla base dei potenziali di minaccia specifici dell'istituto, devono essere condotte **esercitazioni informatiche** basate sul rischio e su scenari. I risultati delle esercitazioni devono essere documentati e riportati in forma adeguata. La portata e il contenuto di tali esercitazioni devono rispettare il principio di proporzionalità. Gli istituti non rilevanti per il sistema dovrebbero effettuare almeno un'esercitazione «table-top» all'anno, intesa come simulazione di uno scenario su carta (esercitazione teorica). 16 4

j. Rischi relativi ai dati critici

L'istituto fintech deve definire le linee guida per la gestione dei rischi relativi ai **dati critici** rilevanti per l'istituto stesso e deve monitorarne il rispetto. I dati critici sono dati che richiedono una protezione particolare e che devono quindi essere definiti dall'istituto in base al rischio. I dati critici possono essere critici sia in termini di riservatezza che di integrità o disponibilità e sono pertanto soggetti a diversi livelli di criticità. 16 5

I dati critici in termini di **riservatezza**, ovvero i dati riservati, sono informazioni aziendali o dati relativi ai clienti o alle persone fisiche che devono essere protetti dall'accesso non autorizzato al fine di tutelare la privacy o la sicurezza di una persona o di un'organizzazione. 16 6

I dati critici in termini di **integrità o disponibilità** devono essere definiti dall'istituto sulla base dei rischi. La criticità di questi dati si riferisce alla capacità dell'istituto di operare in modo efficiente ed efficace (o in generale) di operare. Tali dati critici sono quindi indispensabili per il funzionamento dell'istituto. Esempi di tali «dati critici per la missione» sono, ad esempio, i dati contenuti nei rendiconti finanziari (sia interni che esterni), nelle relazioni normative, nonché i dati utilizzati per i processi decisionali, per l'implementazione tecnica o per la misurazione delle prestazioni aziendali. Se questo tipo di dati viene danneggiato, distrutto o non è più accessibile, l'istituto, le sue unità e i suoi collaboratori potrebbero non essere più in grado di adempiere ai propri compiti. 16 7

- 16 I dati critici devono essere gestiti lungo l'intero **ciclo di vita**. Il ciclo di vita
8 comprende le responsabilità relative ai dati, la raccolta, l'archiviazione, la manutenzione, conservazione (retention), cancellazione e smaltimento. Esso tiene conto inoltre degli aspetti relativi alla produzione, all'arricchimento, al trattamento e alla trasmissione dei dati critici.
- 16 Gli incidenti che compromettono in modo significativo la riservatezza,
9 l'integrità o la disponibilità dei dati critici devono essere segnalati immediatamente alla **FINMA**.
- 17 Nella selezione dei **fornitori di servizi** che trattano dati critici (ovvero
0 qualsiasi forma di gestione degli stessi) o che possono accedervi, occorre attribuire grande importanza alla verifica di due diligence. È necessario definire criteri chiari per la valutazione della gestione dei dati critici da parte dei fornitori di servizi e verificarli prima della stipula del contratto. I fornitori di servizi devono essere monitorati e controllati periodicamente, in base al rischio, nell'ambito del sistema di controllo interno dell'istituto.

k. Gestione della continuità operativa

- 17 Ogni settore operativo e organizzativo rilevante deve identificare, nell'ambito
1 della *Business Impact Analysis* (BIA), i propri processi critici e le risorse necessarie a tal fine (in particolare per quanto riguarda il personale, le strutture (ad es. edifici, infrastrutture delle postazioni di lavoro), le informazioni, i sistemi informatici o l'infrastruttura IT ecc.) e presentarli alla FINMA.
- 17 Per i processi critici, l'istituto deve definire il *Recovery Time Objective* (RTO)
2 e il *Recovery Point Objective* (RPO) in termini di intervalli di tempo e presentarli alla FINMA. Tali parametri devono essere concordati con i fornitori di servizi necessari a tal fine. Il rispetto dell'RTO e dell'RPO deve essere disciplinato da accordi sul livello di servizio (Service Level Agreements) o da contratti, oppure garantito mediante altre procedure, processi e controlli adeguati.
- 17 L'istituto deve definire almeno un *BCP* e presentarlo alla FINMA; tale piano
3 deve descrivere anche le circostanze che ne determinano l'attivazione e i processi decisionali, tenendo conto della perdita di risorse. L'accettazione dei rischi residui deve essere adeguatamente documentata.

L'istituto definisce almeno un *DRP* come parte del BCP. Qualora i processi critici o parti di essi siano esternalizzati, il *DRP* deve tenere conto delle dipendenze esterne, delle disposizioni contrattuali e delle soluzioni alternative. Il *DRP* deve essere rivisto *ad hoc* in caso di modifiche sostanziali, almeno una volta all'anno.

In situazioni di crisi, un **gruppo di crisi** ha il compito di assumere la gestione della crisi fino al ripristino di una situazione regolare. Le circostanze che determinano la crisi, nonché i compiti, le competenze e le responsabilità del gruppo di crisi devono essere definiti in anticipo e l'organizzazione di crisi deve essere adeguata all'attività commerciale e alla struttura geografica dell'istituto. In caso di crisi, deve essere garantita la reperibilità dei responsabili. L'istituto deve sviluppare una **strategia di comunicazione** per la comunicazione interna ed esterna in situazioni di crisi.

L'attuazione del BCP e del *DRP*, nonché l'operatività dell'organizzazione di crisi, devono essere verificate mediante **test periodici**. A tal fine occorre elaborare una pianificazione sistematica che garantisca una copertura regolare. È possibile scegliere diversi approcci di test con intensità ed efficacia variabili, come ad esempio le esercitazioni «table-top».

I test comprendono diversi **scenari** gravi ma plausibili e tengono conto delle dipendenze nel processo di ripristino, comprese quelle da soggetti terzi interni o esterni. A tal fine, occorre illustrare la capacità tecnica di rilevamento nell'ambito del rispettivo scenario, ad esempio gestendo un sistema centrale di *Security Information and Event Management* (SIEM) che offra una visione unitaria degli eventi di sicurezza nell'intero ambiente ICT e consenta così di individuare le minacce e reagire ad esse in modo più efficiente.

Una **rendicontazione** periodica all'organo di direzione supremo e al management fornisce informazioni sulle attività di test e verifica svolte e sui relativi risultati. Essa illustra le priorità stabilite (ad es. la priorità attribuita ai processi critici necessari per l'esecuzione delle funzioni critiche) e le lacune individuate nella copertura di altri processi critici.

1. Rischi derivanti dall'attività transfrontaliera di prestazione di servizi

Se gli istituti o le società del loro gruppo **prestano servizi a livello transfrontaliero** o distribuiscono prodotti finanziari a livello transfrontaliero,

occorre anche rilevare, limitare e monitorare in modo adeguato i rischi derivanti dall'applicazione delle normative estere (diritto fiscale, penale, in materia di riciclaggio di denaro, ecc.) devono essere adeguatamente individuati, limitati e monitorati. La relativa analisi dei rischi deve essere presentata alla FINMA. Per garantire il rispetto delle normative estere, devono essere presentati alla FINMA i relativi manuali per paese.

- 18 Gli istituti sottopongono la propria attività transfrontaliera di prestazione di
0 servizi e la distribuzione transfrontaliera di prodotti finanziari a un'analisi approfondita del quadro giuridico e dei rischi connessi. Sulla base di tale analisi, gli istituti adottano le necessarie **misure** strategiche e organizzative volte all'eliminazione e a minimizzare i rischi, adeguandole costantemente alle mutevoli condizioni quadro. In particolare, dispongono del necessario know-how specifico per ciascun Paese, definiscono modelli di assistenza specifici per ciascun Paese, formano i collaboratori e garantiscono il rispetto delle disposizioni mediante adeguate misure organizzative, direttive, modelli di remunerazione e di sanzione. La relativa direttiva transfrontaliera deve essere presentata alla FINMA.
- 18 Occorre tenere conto anche dei rischi derivanti da gestori patrimoniali
1 esterni, intermediari e altri fornitori di servizi. Nella **selezione e nell'istruzione** di questi partner occorre procedere con la dovuta diligenza.
- 18 Rientrano in questo principio anche le situazioni in cui una filiale, una
2 succursale o un'entità analoga **domiciliata all'estero** di un istituto svizzero fornisce servizi transfrontalieri alla clientela.

m. Resilienza operativa

- 18 L'istituto identifica le proprie funzioni critiche (operazioni o prestazioni
3 strategicamente più importanti) e i relativi livelli di tolleranza alle interruzioni. Questi vengono approvati dall'organo di direzione superiore. Inoltre, l'organo di direzione superiore approva e monitora regolarmente le procedure volte a garantire la **resilienza operativa**. Si tratta della capacità di resistere a shock operativi significativi con il minor impatto negativo possibile e di superarli tempestivamente.
- 18 Nell'ambito della verifica della resilienza operativa, la richiedente deve
4 definire le **funzioni critiche** e indicare una tolleranza all'interruzione più elevata (ad es. 1-5 giorni) per ciascuna funzione critica. Le funzioni critiche

devono essere delimitate dal BCM e occorre definire una *Tolerance for Disruption* di livello superiore.

Su questa base, l'istituto deve stabilire **misure** adeguate per garantire la resilienza operativa, tenendo conto di scenari gravi ma plausibili. In questo contesto è necessario adottare un approccio preventivo con misure mirate, lo sviluppo del modello operativo e un continuo per rendere le funzioni critiche il più resilienti possibile («Resilience by Design»).

4. Ufficio specializzato in materia di riciclaggio di denaro

Gli istituti fintech sono soggetti alla Legge sul riciclaggio di denaro (LRD) (art. 2 cpv. 2 lett. a LRD). Gli **obblighi di diligenza in materia di riciclaggio di denaro** sono disciplinati dal titolo 5 dell'ORD-FINMA (art. 3 cpv. 1 in combinato disposto con l'art. 43a ORD-FINMA). Inoltre, la Circolare FINMA 2016/7 «Identificazione tramite video e online» si applica agli istituti fintech.

Gli istituti fintech devono, tra l'altro, redigere un'**analisi dei rischi di riciclaggio** che comprenda diversi elementi: nell'analisi occorre innanzitutto definire la tolleranza al rischio, escludendo esplicitamente determinati rischi. Inoltre, nell'analisi va specificato in che modo vengono considerati i vari rischi di riciclaggio. Infine, l'istituto fintech deve definire indicatori e soglie per poter dimostrare il rispetto della propria strategia aziendale e della propria politica di rischio, nonché il loro sviluppo nel corso degli anni. L'analisi dei rischi contiene quindi le informazioni essenziali sulla gestione prevista dei rischi di riciclaggio.

Dal punto di vista dei contenuti, la struttura dell'analisi dei rischi di riciclaggio dipende fortemente dalle effettive attività commerciali, sia dal punto di vista oggettivo che geografico, dell'istituto fintech. Come categorie di rischio significative possono in parte fungere le seguenti: a. struttura della clientela (rischi paese, segmenti di clientela, vicinanza relazionale con il cliente), b. tipo di rapporto con il cliente/strutture complesse, c. attività commerciali (prodotti e servizi), d. rapporti d'affari con rischi elevati (PEP, società di comodo), e. rischi legati alle transazioni e simili.

Gli intermediari finanziari devono disporre di una **funzione adeguata** per la lotta contro il riciclaggio di denaro e il finanziamento del terrorismo (compresa l'elusione delle sanzioni). Le persone incaricate di tali compiti devono essere adeguatamente formate e disporre delle risorse necessarie per

poter svolgere adeguatamente la propria funzione. Le relative norme interne da osservare devono essere documentate in forma adeguata e messe a disposizione dei collaboratori incaricati di tali compiti. A tal fine, le disposizioni legali applicabili devono essere attuate a livello interno.

190 Gli istituti fintech hanno la possibilità di beneficiare di **agevolazioni organizzative** nell'ambito del servizio specializzato in materia di riciclaggio di denaro, a condizione che l'istituto soddisfi anche i requisiti per le agevolazioni nel settore della compliance e della gestione dei rischi (art. 14e cpv. 5 OB) e che l'obiettivo della lotta contro il riciclaggio di denaro e il finanziamento del terrorismo non sia in contrasto con tali agevolazioni (cfr. art. 75a ORD-FINMA). A seconda del rischio di riciclaggio, la FINMA può concedere ulteriori agevolazioni o disporre inasprimenti (cfr. art. 3 cpv. 2 ORD-FINMA).

5. Documentazione e processi

19 Di norma, i richiedenti devono presentare come documentazione le linee guida relative ai seguenti argomenti (regolamenti del Consiglio di amministrazione o direttive della Direzione) da presentare come **documentazione**:

- organizzazione generale e competenze in materia di gestione dei rischi (spesso descritte nell'OGR);
- strategia aziendale e politica dei rischi;
- analisi dei rischi;
- gestione generale dei rischi;
- matrice di controllo generale (comprese competenze, periodicità e contenuti dei controlli) ;
- rischi operativi (compresi rischi ICT/cibernetici, rischi relativi ai dati critici, protezione e sicurezza dei dati e gestione della continuità operativa [BCM]);
- conformità in generale;
- riciclaggio di denaro e sanzioni in particolare;
- in caso di attività all'estero: operazioni transfrontaliere, compresi i manuali per paese;

- esternalizzazioni (e relativi contratti di esternalizzazione) ;
- Custodia dei depositi del pubblico e monitoraggio della soglia di 100 milioni di CHF;
- Comportamento dei collaboratori;
- Gestione dei patrimoni non reclamati (cfr. art. 37l e art. 37m LBCR nonché art. 45 segg. OB);
- in caso di applicabilità della FIDLEG: comportamento/condotta nei confronti dei clienti.

6. Prevenzione dei conflitti di interesse

Gli istituti fintech devono adottare adeguate misure organizzative per evitare i **conflitti di interesse** che potrebbero insorgere nella prestazione dei loro servizi, ovvero per escludere che i clienti subiscano un pregiudizio a causa di tali conflitti. Qualora non sia possibile escludere un conflitto di interesse, questo deve essere reso pubblico (art. 14g OB) e i clienti devono esserne informati di conseguenza. Gli interessi propri dei titolari dell'autorizzazione e dei loro collaboratori non devono essere in contrasto con gli interessi dei clienti. Allo stesso modo, gli interessi dei clienti non devono entrare in conflitto tra loro.

D. Requisiti finanziari (cpv. 3 lett. c)

1. Piano aziendale

La richiedente deve presentare un **piano aziendale** comprensivo di bilancio preventivo (bilancio, conto economico) per i prossimi tre esercizi, con scenari ottimistico, realistico e pessimistico. La pianificazione della liquidità per il primo esercizio deve essere effettuata in base allo scenario pessimistico del piano aziendale (su base mensile).

Gli istituti fintech devono disporre di un **modello di business** che garantisca l'adempimento indipendente e duraturo dei propri obblighi finanziari. Occorre evitare che i criteri di autorizzazione siano fissati a un livello troppo basso e che la propensione al rischio sia eccessiva. Qualora un istituto, per motivi strutturali, non sia in grado di generare utili e possa esistere solo grazie a sovvenzioni degli azionisti (a fondo perduto), sussiste una situazione irregolare che mette in discussione l'idoneità all'autorizzazione. In tal caso, la

sopravvivenza dell'istituto dipende esclusivamente dalla solvibilità e dalla volontà dei proprietari economici, il che costituisce un rischio inaccettabile sia dal punto di vista della tutela dei creditori che da quello della continuità operativa. Anche un'eccedenza di fondi propri e la determinazione dei proprietari economici a coprire, anno dopo anno, le perdite operative sostenute, in modo da non far sorgere alcun pericolo immediato per i creditori, non costituiscono, sotto questi aspetti una redditività insufficiente di lunga durata. Per dimostrare di poter soddisfare tali requisiti, la richiedente deve in particolare presentare gli scenari economici realistici e fondati menzionati.

- 19 La **vigilanza** della FINMA non garantisce, in questo senso, il successo
5 commerciale degli istituti sottoposti a vigilanza, ma è finalizzata alla tutela dei clienti. Nell'ambito della procedura di autorizzazione, la FINMA verifica che i piani aziendali e i piani di finanziamento siano plausibili. Tale verifica è tanto più importante in quanto i clienti di soggetti ai sensi dell'art. 1b LBCR non sono tutelati in caso di loro fallimento (in particolare, i loro crediti sono subordinati a quelli salariali) e i fallimenti in questo settore non sono rari e possono verificarsi anche nella fase iniziale.
- 19 Nella relativa **analisi** del modello di business occorre tenere conto, tra l'altro,
6 dei seguenti punti:
- identificazione dei rischi principali del modello di business;
 - verifica della capacità dell'istituto di adattarsi a eventuali mutamenti delle circostanze;
 - analisi delle risorse finanziarie disponibili e delle altre risorse necessarie per l'attuazione della strategia;
 - valutazione della strategia e della propensione al rischio dell'istituto;
 - considerazione del contesto di mercato e di attività e confronto delle ambizioni di crescita della società con quelle di altri operatori;
 - verifica della realizzabilità o della plausibilità delle ipotesi del piano aziendale;
 - verifica della redditività di un istituto al fine di garantire un adeguato rendimento del capitale e assicurare la continuità dell'attività aziendale dell'istituto (compresa un'adeguata copertura dei costi di finanziamento (capitale di terzi e capitale proprio) e dei costi operativi).

Se l'istituto fintech oggetto di valutazione fa parte di un **gruppo**, i criteri di cui sopra devono essere verificati non solo a livello del singolo istituto, ma anche a livello di gruppo. 19 7

2. Liquidità

Gli istituti fintech devono disporre di adeguate **risorse finanziarie** (art. 1b cpv. 3 lett. c LBCR). L'ambito di attività e la sua estensione geografica devono corrispondere alle possibilità finanziarie dell'istituto fintech (art. 14b cpv. 2 OB). 19 8

Per motivi di rischio, la FINMA richiede che un istituto fintech disponga, al momento del rilascio dell'autorizzazione, di mezzi liquidi sufficienti a coprire almeno i costi fissi nella fase iniziale, tenendo conto di eventuali proventi. A tal fine, l'istituto fintech deve presentare una **pianificazione della liquidità** (su base mensile) e, come requisito per l'autorizzazione, di presentare prove (estratto conto bancario ecc.) relative all'attuale disponibilità di liquidità. 19 9

Per garantire la solvibilità, l'istituto fintech deve integrare i **rischi di liquidità** nella propria gestione dei rischi e monitorarli costantemente nell'ambito del sistema di controllo interno. 20 0

3. Capitale minimo

Per ottenere l'autorizzazione, un istituto fintech deve dimostrare di disporre del capitale minimo stabilito dal Consiglio federale, interamente versato (art. 1b cpv. 1 in combinato disposto con l'art. 3 cpv. 2 lett. b LBCR). Gli istituti fintech devono disporre di un **capitale minimo** pari al 3 per cento dei depositi del pubblico raccolti e delle attività basate su criptovalute detenute in custodia collettiva, con un importo minimo di CHF 300'000. Esso deve essere interamente versato e deve essere mantenuto in modo permanente. 20 1

Il capitale minimo deve essere utilizzato per lo **scopo** dell'impresa. Non può quindi essere prestato a partecipanti qualificati o a persone fisiche o giuridiche a loro vicine, né essere investito in partecipazioni da essi controllate (art. 17a cpv. 1 OB). Questa limitazione delle possibilità di investimento mira a ridurre il rischio di svuotamento (rischio di frode) dell'impresa. Le disposizioni dell'ORD e dell'Orli non sono applicabili in assenza di trasformazione delle scadenze (art. 17a cpv. 3 OB). 20 2

- 20 Sussistono tuttavia alcuni **rischi di liquidità e di controparte**. Pertanto,
3 anche per le persone di cui all'art. 1b LBCR deve essere garantito che dispongano di mezzi finanziari sufficienti per poter sostenere i propri rischi. Il capitale minimo non deve solo garantire una certa tutela dei depositi, ma soprattutto assicurare un'adeguata dotazione organizzativa e tecnica dell'istituto.
- 20 La FINMA può stabilire, in singoli casi, **requisiti di fondi propri più elevati**,
4 qualora ciò appaia necessario in ragione dei rischi connessi all'attività (art. 17a cpv. 2 OB) . La calibrazione dei requisiti patrimoniali deve garantire un'applicazione equa e paritaria tra i diversi modelli di business. Il capitale supplementare ai sensi dell'art. 17a cpv. 2 OB deve consentire una durata minima di sopravvivenza degli istituti autorizzati.
- 20 Per **dimostrare** il rispetto dei requisiti finanziari, la richiedente deve
5 presentare le seguenti informazioni:
- documentazione adeguata che attesti il rispetto dei requisiti di capitale minimo e una descrizione di come venga garantito il rispetto dei requisiti minimi in caso di aumento dei depositi del pubblico;
 - andamento previsto del capitale minimo in base al piano aziendale, comprese le informazioni sulle fonti di finanziamento.

E. Garanzia (cpv. 3 lett. d)

- 20 Le persone incaricate di funzioni organiche – ai tre livelli di azionariato
6 qualificato, direzione e consiglio di amministrazione – devono godere di buona reputazione e offrire **garanzia di un'attività commerciale irrepreensibile** (art. 1b cpv. 3 lett. d LBCR) (le cosiddette «persone di garanzia») . La verifica della garanzia comprende due aspetti: l'idoneità professionale («fitness») per la funzione specifica e l'integrità personale («properness») di tali persone. Ai fini della verifica della garanzia e della buona reputazione, insieme alla domanda relativa alle persone che offrono garanzia vengono richiesti informazioni e documenti (cfr. art. 8 OB).
- 20 Per dimostrare il rispetto dei requisiti richiesti ai membri dell'organo
7 incaricato dell'amministrazione e della direzione, devono essere presentati i seguenti **documenti**:
- Dati personali;

- Copia di un documento di identità valido (copia del passaporto o della carta d'identità firmata e datata);
- Copia del permesso di soggiorno o di stabilimento per i cittadini stranieri (copia firmata e datata);
- estratto del casellario giudiziario (non più vecchio di 3 mesi);
- estratto del casellario giudiziario dello Stato di residenza precedente e/o di origine per i cittadini stranieri che risiedono in Svizzera da meno di 5 anni (non più vecchio di 3 mesi);
- estratto del registro delle esecuzioni o attestato equivalente (non più vecchio di 3 mesi);
- curriculum vitae firmato dall'interessata (comprensivo di informazioni sulla formazione iniziale e continua e di almeno due referenze); elenco e descrizione delle attività professionali e dei mandati svolti in passato e attualmente, comprese le annate e le date);
- contratto con la richiedente (firmato e datato);
- dichiarazione relativa ai procedimenti pendenti e conclusi (modulo B1, firmato e datato);
- dichiarazione relativa alle partecipazioni qualificate (modulo B3, firmato e datato);
- dichiarazione relativa ad altri mandati (modulo B3, firmato e datato).

A tal fine, la FINMA richiede alla richiedente (utilizzando i **moduli** da essa prestabiliti) di presentare le seguenti informazioni **relative alle partecipazioni, ovvero all'azionariato:** 20
8

- capitale sociale (struttura, ripartizione, valore nominale, liberazione ecc.);
- elenco di tutti i soggetti con una partecipazione diretta o indiretta pari o superiore al 5 per cento (fino all'avente diritto economico, con indicazione dei diritti di voto e della quota di capitale);
- rappresentazione grafica di tutti i soggetti con partecipazioni qualificate, dirette o indirette, fino ai titolari effettivi (compresa l'indicazione dell'entità della rispettiva partecipazione), suddivisa per quote di diritti di voto e di capitale;

- informazioni su eventuali accordi nonché su altre possibilità di controllo o di influenza determinante; Devono essere presentati documenti quali, ad esempio, accordi di vincolo tra azionisti o contratti di investimento;
- Dichiarazione relativa ai titolari di partecipazioni qualificate (modulo A1; da presentare da parte del richiedente);
- Allegato alla dichiarazione relativa ai titolari di partecipazioni qualificate (modulo A2; per ciascun partecipante qualificato; da presentare da parte del richiedente).

20 **I partecipanti qualificati** devono anch'essi godere di buona reputazione e
9 garantire che la loro influenza non si ripercuota a danno di un'attività commerciale prudente e solida. Non devono tuttavia essere indipendenti dalla direzione aziendale. È considerato partecipante qualificato chi detiene almeno il **10 per cento** dei voti o del capitale o chi può influenzare in modo determinante l'attività commerciale in altro modo (art. 14d cpv. 3 OB). La variante dell'influenza «in altro modo» non serve solo a chiarire lo scopo della norma, ma ha anche un significato autonomo. In tal modo si intendono cogliere ulteriori influenze di fatto e di diritto, indipendentemente dalle soglie.

21 A partire da una partecipazione superiore al **5 per cento**, a causa della
0 possibile influenza in altro modo, sono richiesti i documenti giustificativi elencati nelle .

21 I documenti giustificativi richiesti per le persone fisiche in qualità di
1 **partecipanti qualificati**, direttamente o indirettamente, comprendono:

- dati personali;
- copia di un documento di identità valido (copia del passaporto o della carta d'identità firmata e datata dal titolare);
- estratto del casellario giudiziale (non più vecchio di 3 mesi);
- estratto del casellario giudiziale dello Stato di residenza precedente e/o di origine per i cittadini stranieri che risiedono in Svizzera da meno di 5 anni (non più vecchio di 3 mesi);
- estratto del registro delle esecuzioni o attestato equivalente (non più vecchio di 3 mesi);

- curriculum vitae firmato dall'interessato (comprensivo di informazioni sulla formazione iniziale e continua e di almeno due referenze, elenco e descrizione delle attività professionali e dei mandati svolti in passato e attualmente, con indicazione di anni e date);
- dichiarazione che indichi se la partecipazione qualificata è detenuta per conto proprio o in qualità di fiduciario per conto di terzi e se il partecipante qualificato ha concesso opzioni o diritti simili relativi a tale partecipazione (moduli «Dichiarazione dei soggetti direttamente/indirettamente qualificati», firmati e datati);
- dichiarazione relativa ai procedimenti pendenti e conclusi (modulo B1, firmato e datato);
- dichiarazione sulle partecipazioni qualificate (modulo B2, firmato e datato).

I documenti giustificativi richiesti per le **persone giuridiche** in qualità di soggetti qualificati, direttamente o indirettamente, comprendono: 21
2

- descrizione dettagliata dell'organizzazione, delle attività commerciali, della situazione finanziaria (compreso l'ultimo bilancio annuale, se disponibile) e, se del caso, della struttura del gruppo;
- estratto del registro delle esecuzioni o attestazione equivalente (non più vecchio di 3 mesi);
- estratto del registro di commercio o attestazione corrispondente;
- dichiarazione che indichi se la partecipazione qualificata è detenuta per conto proprio o in qualità di fiduciario per conto di terzi e se il partecipante qualificato ha concesso opzioni o diritti simili relativi a tale partecipazione (moduli A3/A4, firmati e datati);
- Dichiarazione relativa ai procedimenti pendenti e conclusi (modulo B1, firmato e datato);
- Dichiarazione sulle partecipazioni qualificate (modulo B2, firmato e datato).

F. Rendicontazione e revisione contabile (cpv. 4, lettere a, b e c)

La **rendicontazione** e la revisione del conto annuale si basano esclusivamente sulle disposizioni del CO (art. 1b cpv. 4 lett. a LBCR), senza 21
3

che sia possibile rinunciare alla revisione limitata (nessun «opting-out» ai sensi dell'art. 727a cpv. 2-5 CO) (art. 1b cpv. 4 lett. b LBCR) . Qualora i depositi del pubblico non siano separati dal capitale proprio, deve essere effettuata una revisione ordinaria (art. 14f cpv. 1 lett. b OFin). Idealmente, l'istituto effettua una revisione ordinaria ai sensi dell'art. 727 CO.

- 21 Gli istituti fintech devono incaricare una **società di revisione** autorizzata di
4 effettuare la revisione prudenziale ai sensi dell'art. 24 LLFINMA (art. 1b cpv. 4 lett. c LBCR). A tal fine, devono designare una società di revisione autorizzata ai sensi dell'art. 9a LSR (cfr. art. 24 cpv. 1 lett. a LFINMA). Alla domanda di autorizzazione devono essere allegate una dichiarazione di accettazione della società di revisione prudenziale nonché un questionario compilato sui servizi delle società di revisione autorizzate, disponibile sul sito web della FINMA.

G. Obblighi di informazione (cpv. 4, lett. d)

- 21 Le disposizioni relative ai depositi privilegiati e al pagamento immediato (art.
5 37a e art. 37b LBCR) (garanzia dei depositi) **non si applicano** ai depositi del pubblico e agli attivi basati su criptovalute raccolti da un istituto fintech. Prima dell'accettazione dei depositi, i depositanti devono essere informati della **mancanza di garanzia dei depositi e della mancanza di protezione in caso di fallimento**, nonché delle possibili conseguenze (art. 1b cpv. 4 lett. d LBCR) .
- 21 Ai sensi dell'art. 7a cpv. 1 OB, i clienti devono essere informati per iscritto o in
6 un'altra **forma documentabile** (su un documento separato, all'interno della documentazione relativa al modello di business o anche separatamente via e-mail) in merito all'assenza di garanzia dei depositi, nonché al modello di business degli istituti fintech, ai loro servizi e ai rischi connessi alle tecnologie utilizzate.
- 21 I clienti devono essere informati in modo tale da disporre, **prima della**
7 **conclusione del contratto**, di tempo sufficiente per comprendere le informazioni ai fini della stipula del contratto (art. 7a cpv. 2 OB). Una semplice informazione tramite le condizioni generali di contratto non è sufficiente (art. 7a cpv. 3 OB).
- 21 Se le informazioni vengono messe a disposizione **per via elettronica**, le
8 persone di cui all'art. 1b della LBCR devono garantire che esse possano essere consultate, scaricate e salvate su un supporto durevole in tutte le lingue

(ufficiali) rilevanti per i clienti destinatari (art. 7a cpv. 4 OB). Sono considerati supporti durevoli la carta e qualsiasi altro mezzo che consenta la memorizzazione e la riproduzione inalterata di un'informazione (art. 7a cpv. 5 OB).

La richiedente deve presentare alla FINMA i dati relativi alle informazioni fornite ai clienti ai sensi dell'art. 7a dell'Ordinanza sulle banche. A tal fine, di norma, devono essere presentati il testo corrispondente e il relativo **processo di onboarding**, comprese le schermate delle singole fasi. Le informazioni relative ai rischi connessi al modello di business, ai servizi e alle tecnologie utilizzate devono essere dettagliate. Anche l'avviso relativo alla mancata applicazione delle disposizioni sui depositi privilegiati (art. 37a LBCR), sul pagamento immediato (art. 37b LBCR) e sulla garanzia dei depositi (art. 37h segg. LBCR deve essere completa ed essere messa in evidenza. Dal punto di vista procedurale, l'informazione deve essere strutturata in modo tale che, in caso di mancato consenso, il processo di onboarding del cliente venga interrotto. Un semplice riferimento all'art. 7a OB non è in ogni caso sufficiente. I clienti devono acconsentire attivamente all'informazione (ad es. spuntando una casella con un clic del mouse).

V. CASI PARTICOLARI (COMPRESI I CPV. 5 E 6)

A. Possibile aumento della soglia per i depositi del pubblico da parte della FINMA (cpv. 5 e 6)

Se i depositi del pubblico superano la soglia di 100 milioni di CHF, ciò deve essere comunicato alla FINMA entro 10 giorni e, entro 90 giorni (fatto salvo il cpv. 5), deve essere presentata una **domanda di autorizzazione bancaria** ai sensi dell'art. 1a LBCR (art. 1b cpv. 6 LBCR). Non si ravvisa alcuna necessità di questa disposizione transitoria, poiché una persona ai sensi dell'art. 1b LBCR è comunque sottoposta alla vigilanza della FINMA e intrattiene con essa uno scambio regolare, cosicché in tale contesto è possibile rilevare tempestivamente e senza difficoltà l'avvicinarsi alla soglia di CHF 100 milioni.

Il Consiglio federale può adeguare l'importo di **CHF 100 milioni** tenendo conto della competitività e della capacità di innovazione della piazza finanziaria svizzera (art. 1b cpv. 2 LBCR). In casi singoli motivati, anche la FINMA ha la possibilità di derogare al limite massimo di CHF 100 milioni: in

casi particolari, essa può infatti dichiarare applicabili i capoversi 1–4 anche a soggetti che raccolgono a titolo professionale depositi del pubblico per importi superiori a CHF 100 milioni o che si propongono pubblicamente di non investirli né di correntarli e di garantire la tutela dei clienti mediante misure speciali (art. 1b cpv. 5 LBCR).

B. Combinazione con altre categorie di autorizzazione

22 Una combinazione tra l'attività di un istituto fintech e quella di **società di**
2 **intermediazione mobiliare** non è in linea di principio esclusa. Lo stesso vale per l'attività di **gestore patrimoniale**, sebbene sussistano diverse questioni di coordinamento normativo:

- in particolare, occorre tenere presente che l'autorizzazione fintech non rientra nella **cascata autorizzativa** (cfr. art. 6 LIsFi);
- in caso di combinazione di categorie di autorizzazione, si applicano i **requisiti patrimoniali** più elevati delle due categorie di autorizzazione;
- in caso di combinazione dell'autorizzazione fintech con quella di società di intermediazione mobiliare, la difficoltà operativa risiede infine nel diverso trattamento dei depositi: mentre per gli istituti fintech non esiste una garanzia dei depositi (art. 1b cpv. 4 lett. d LBCR), i clienti delle società di intermediazione mobiliare che gestiscono conti di regolamento beneficiano della **garanzia dei depositi**, il che richiede una separazione dei rispettivi conti di denaro. Per i soggetti di cui all'art. 1b LBCR, la soluzione più adeguata dovrebbe quindi essere quella di esercitare un'eventuale attività di negoziazione per conto dei clienti tramite una persona giuridica autonoma.

C. Vigilanza consolidata

22 Alle persone di cui all'art. 1b LBCR si applicano per analogia le disposizioni
3 della LBCR in materia di vigilanza consolidata, fatte salve le norme speciali di cui all'art. 1b cpv. 1 LBCR. Ciò vale anche per il diritto in materia di consolidamento bancario di cui agli art. 3b segg. LBCR e agli art. 21 segg. Oban. Se un soggetto ai sensi dell'art. 1b LBCR fa parte di un gruppo finanziario, l'autorizzazione può essere subordinata a un'adeguata **vigilanza consolidata** da parte di un'autorità di vigilanza sui mercati finanziari (art. 1b cpv. 1 in combinato disposto con l'art. 3b LBCR).

La **Circolare FINMA 2025/4** «Vigilanza consolidata dei gruppi finanziari ai sensi della LBCR e della LIsFi» illustra la prassi dell'autorità di vigilanza in materia di assoggettamento alla vigilanza consolidata, nonché in merito alla sua portata e al suo contenuto. Per analogia, la circolare si rivolge anche ai gruppi finanziari dominati da persone ai sensi dell'art. 1b LBCR e alle persone ai sensi dell'art. 1b LBCR che fanno parte di un gruppo finanziario (art. 1b cpv. 1 in combinato disposto con l'art. 3c cpv. 1 LBCR) .

La FINMA può quindi esigere una vigilanza consolidata sul gruppo in caso di **situazioni che riguardano il gruppo**. Qualora altre autorità estere rivendichino contemporaneamente la vigilanza totale o parziale sul gruppo finanziario, la FINMA, nel rispetto delle proprie competenze, concorda con esse le competenze, le modalità e l'oggetto della vigilanza sul gruppo. Prima di prendere una decisione, essa sente le imprese del gruppo finanziario costituite in Svizzera (art. 3d cpv. 2 LBCR).

Ai sensi della presente disposizione, si considera **gruppo finanziario** un insieme di due o più imprese qualora: a) almeno un'impresa operi in qualità di persona ai sensi dell'art. 1b LBCR o sia titolare di un'autorizzazione fintech; b) esse operino prevalentemente nel settore finanziario; e c) esse costituiscano un'unità economica *oppure*, in base ad altre circostanze, si possa presumere che una o più società soggette a vigilanza individuale siano giuridicamente obbligate o di fatto costrette a prestare assistenza alle società del gruppo (art. 1b cpv. 1 in combinato disposto con l'art. 3c cpv. 1 LBCR).

Un **obbligo di sostegno** giuridico o di fatto ai sensi dell'art. 21 cpv. 2 OB può derivare in particolare dalle seguenti circostanze:

- interconnessioni strategiche, di personale, organizzative o finanziarie;
- cooperazioni e dipendenze;
- l'utilizzo di una ragione sociale comune;
- una presenza unitaria sul mercato; oppure
- da dichiarazioni di patronato, «keep-well agreements» o garanzie simili.

Le fattispecie espressamente menzionate non sono esaustive. Pertanto, anche altri legami possono dar luogo a un obbligo di sostegno di fatto, qualora da essi possa derivare per terzi l'impressione di un **sistema integrato**. Quanto più elevata è la quota di partecipazione, tanto minori possono essere gli altri

elementi di collegamento per giustificare, nella valutazione complessiva, l'inclusione nella vigilanza consolidata.

- 22 Ai sensi dell'art. 4 cpv. 1 OB, opera nel **settore finanziario** chi: a) fornisce o
9 media servizi per operazioni finanziarie, in particolare esercita, per conto proprio o di terzi, l'attività di raccolta di depositi o di concessione di crediti, il commercio di valori mobiliari, l'attività di investimento di capitale o la gestione patrimoniale, oppure accetta valori patrimoniali basati su criptovalute ai sensi dell'art. 5a OB; b) detiene partecipazioni qualificate prevalentemente in imprese operanti nel settore finanziario (società holding); oppure c) è una società del gruppo di rilievo ai sensi dell'art. 3a OB.
- 23 Le **attività** elencate espressamente nell'art. 4 cpv. 1 lett. a OB non
0 costituiscono un elenco esaustivo. Pertanto, anche altre attività commerciali possono costituire attività nel settore finanziario. Tra queste rientrano in particolare il leasing finanziario, il factoring, le operazioni con carte di credito, la partecipazione a emissioni, nonché la custodia di titoli, i servizi di pagamento e l'emissione e la custodia di mezzi di pagamento (compresi i token di pagamento). Ai fini della vigilanza consolidata, le società del gruppo che esercitano attività puramente commerciali, industriali o amministrative non sono considerate operanti nel settore finanziario.
- 23 Le imprese costituiscono un'**unità economica** quando una di esse detiene,
1 direttamente o indirettamente, più della metà dei voti o del capitale delle altre imprese, oppure le controlla in altro modo (art. 21 cpv. 1 OB). Ai sensi dell'art. 21 cpv. 2 OB, un obbligo di assistenza può derivare in particolare da: a) interconnessioni a livello di personale o finanziario; b) l'utilizzo di una ragione sociale comune; c) una presenza unitaria sul mercato; oppure d) dichiarazioni di patronato. Le società del gruppo sono imprese collegate da un'unità economica o da un obbligo di assistenza (art. 22 OB).
- 23 L'inclusione di una società nella vigilanza consolidata può essere determinata
2 anche in assenza di una partecipazione di maggioranza («controllata in altro modo»), purché ulteriori elementi di natura giuridica o di fatto indichino l'esistenza di un sistema interconnesso. Sono considerati tali, in particolare, i legami e le dipendenze a livello di personale, organizzativo, finanziari o commerciali, **nonché dipendenze**. Se una persona ai sensi dell'art. 1b LBCR è controllata da una o più persone fisiche che controllano altre società soggette alla vigilanza della FINMA o altre società significative operanti nel

settore finanziario, in determinate circostanze si ha un cosiddetto gruppo finanziario *de facto*, che deve essere sottoposto a vigilanza consolidata.

La FINMA può assoggettare un gruppo finanziario alla **vigilanza di gruppo** qualora esso: a) gestisca in Svizzera una persona organizzata secondo il diritto svizzero ai sensi dell'art. 1b LBCR; oppure b) sia effettivamente diretto dalla Svizzera (art. 1b cpv. 1 in combinato disposto con l'art. 3d cpv. 1 LBCR). La vigilanza di gruppo esercitata dalla FINMA comprende tutte le società del gruppo operanti nel settore finanziario (art. 23 cpv. 1 OB). ^{23 3}

In casi motivati, la FINMA può **escludere** dalla vigilanza consolidata le società del settore finanziario appartenenti al gruppo o dichiararne l'applicabilità solo parziale, in particolare se una società del gruppo è irrilevante ai fini della vigilanza consolidata (art. 23 cpv. 2 OFin). La FINMA può **includere**, in tutto o in parte, nella vigilanza consolidata un'impresa del settore finanziario che sia controllata da un gruppo finanziario sottoposto alla vigilanza della FINMA insieme a terzi (art. 23 cpv. 3 OB). ^{23 4}

Sulla base di considerazioni relative alla tutela degli investitori e dei creditori, la FINMA applica, nel caso di strutture di gruppo che comprendono istituti fintech, il **principio della vigilanza consolidata**, tenendo conto dei rischi specifici del singolo caso. ^{23 5}

La definizione del **perimetro di consolidamento** ai fini della vigilanza consolidata della FINMA avviene di concerto con l'autorità di vigilanza estera competente ai sensi dell'art. 3d cpv. 2 LBCR e comprende in particolare la determinazione di quale sia l'autorità di vigilanza competente in via primaria (*Lead Regulator*). Inoltre, è parte integrante della vigilanza consolidata che tutte le autorità di vigilanza interessate si accordino tra loro in merito alle competenze e alle modalità di collaborazione. Le modalità della collaborazione in materia di vigilanza e dello scambio di informazioni vengono stabilite caso per caso o anche in via generale tra le autorità di vigilanza. In tal modo si garantisce che non sorgano né lacune né duplicazioni. ^{23 6}

Per affrontare i rischi a livello di gruppo, la FINMA può, applicando il principio di proporzionalità, anziché ricorrere alla vigilanza consolidata o al rifiuto dell'autorizzazione, disporre misure strutturali preventive adeguate per la **separazione** (*ring fencing*) o ulteriori misure (ad es. adeguamento della struttura del gruppo). ^{23 7}

- 23 In caso di controllo estero, tuttavia, occorre in ogni caso ottenere
8 l'approvazione delle competenti **autorità di vigilanza estere** (cfr. art. 1b cpv. 1 in combinato disposto con l'art. 3^{bis} cpv. 1^{bis} LBCR). La vigilanza consolidata deve in linea di principio riguardare tutti gli aspetti oggetto di vigilanza (consolidamento qualitativo e quantitativo).
- 23 In caso di attività di gruppo, il richiedente deve:
9
- presentare un **organigramma** del gruppo con indicazioni sulle autorizzazioni ai sensi della normativa sui mercati finanziari già esistenti o previste, una rappresentazione grafica nonché le quote di diritti di voto e di capitale; nonché
 - una descrizione dettagliata di tutti gli **elementi di collegamento** strategici, relativi al personale, organizzativi o finanziari tra il richiedente e tutte le società del gruppo.

D. Situazioni transfrontaliere

- 24 Gli istituti fintech possono operare all'estero, essere sotto controllo straniero
0 e/o appartenere a un gruppo finanziario estero. Si pone inoltre la questione della reciprocità e del riconoscimento delle categorie di autorizzazioni estere come equivalenti all'autorizzazione fintech e, di conseguenza, la questione della possibilità di aprire succursali e rappresentanze.

1. Attività all'estero (*outbound*)

- 24 Gli istituti fintech possono svolgere un'**attività all'estero** attiva o anche solo
1 passiva, nel senso di una prestazione transfrontaliera di servizi. Ogni attività all'estero comporta, per gli istituti fintech, un aumento dei rischi connessi all'attività commerciale e un ampliamento dell'ambito di compliance. Di conseguenza, i rischi derivanti dall'applicazione delle normative estere (legislazione fiscale, penale, antiriciclaggio, ecc.) devono essere adeguatamente individuati, classificati e limitati mediante un'analisi dei rischi (misure strategiche e organizzative, know-how, modelli di servizio per paese, formazione, selezione dei partner) e controllati (mediante direttive, modelli di remunerazione e sanzioni).
- 24 Un'**attività all'estero attiva** presuppone di norma, in base al diritto estero,
2 una sorta di organizzazione amministrativa locale dell'istituto fintech all'estero. Di conseguenza, gli istituti fintech organizzati secondo il diritto

svizzero devono presentare una notifica alla FINMA prima di costituire all'estero una filiale, una succursale, un'agenzia o una rappresentanza (art. 1b cpv. 1 in combinato disposto con l'art. 3 cpv. 7 LBCR). La notifica che un istituto fintech deve presentare alla FINMA prima di avviare l'attività all'estero deve contenere tutte le informazioni e i documenti necessari per la valutazione dell'attività, in particolare: a) un piano aziendale che descriva in particolare la natura delle operazioni previste e la struttura organizzativa, b) l'indirizzo della sede estera, c) i nomi delle persone incaricate dell'amministrazione e della direzione, d) la società di revisione, e) l'autorità di vigilanza nel Paese ospitante (art. 20 cpv. 1 OB). L'istituto fintech deve inoltre comunicare la cessazione o qualsiasi modifica sostanziale dell'attività all'estero, nonché il cambio della società di revisione o dell'autorità di vigilanza (art. 20 cpv. 2 OB).

Anche nel caso di un'**attività all'estero puramente passiva**, questa deve essere illustrata nell'OGR mediante una descrizione precisa, sia dal punto di vista oggettivo che territoriale, dell'ambito di attività (cfr. art. 1b cpv. 3 lett. a LBCR; art. 14b cpv. 1 OB). Ne derivano requisiti più rigorosi per l'organizzazione amministrativa interna e per la corporate governance. In tal senso, è richiesto che i relativi rischi e controlli siano affrontati nell'ambito dell'organizzazione e della documentazione della gestione dei rischi e della compliance. Ciò comprende di norma, in particolare, anche una direttiva transfrontaliera che includa i cosiddetti «Country Manuals» dei paesi in cui si opera. Qualora istituti fintech già autorizzati intendano avviare una nuova attività passiva all'estero, ciò costituisce una modifica sostanziale dei presupposti di autorizzazione e deve pertanto essere preventivamente autorizzato (cfr. art. 8a cpv. 2 OB). Non è possibile avviare l'attività nell'OGR a titolo provvisorio.

2. Controllo estero

La FINMA può subordinare l'autorizzazione alla costituzione di un istituto fintech, che debba essere organizzato secondo il diritto svizzero, ma sul quale sussista tuttavia, ad esempio, un **controllo estero** (cfr. a tal proposito l'art. 3^{bis} cpv. 3 LBCR) da parte, ad esempio, di azionisti o società del gruppo con sede all'estero, anche ai seguenti requisiti (art. 1b cpv. 1 in combinato disposto con l'art. 3^{bis} cpv. 1 LBCR):

1. dalla garanzia della **reciprocità** da parte degli Stati in cui gli stranieri con partecipazioni qualificate hanno il domicilio o la sede (cfr. art. 19 cpv. 1 OB), purché non vi siano obblighi internazionali in senso contrario (cfr. art. 3^{quater} LBCR); nonché

2. dall'utilizzo di una **ragione sociale** che non indichi o non lasci supporre il carattere svizzero dell'istituto fintech.

- 24 Lo stesso vale per gli istituti fintech che, dopo la loro costituzione, sono
5 controllati da soggetti esteri o qualora cambino i soggetti esteri titolari di partecipazioni qualificate (art. 1b cpv. 1 in combinato disposto con l'art. 3^{ter} cpv. 1–2 LBCR) . Le domande relative a tali **autorizzazioni supplementari** in qualità di istituto fintech a controllo estero devono contenere le indicazioni di cui all'art. 8 OB (art. 18 OB).

3. Rappresentanze (*inbound*)

- 24 In applicazione del rinvio generale per analogia di cui all'art. 1b cpv. 1 LBCR,
6 le disposizioni della LBCR si applicano per analogia alle succursali istituite in Svizzera o ai rappresentanti designati da «persone straniere ai sensi dell'art. 1b LBCR» (art. 1b cpv. 1 in combinato disposto con l'art. 2 cpv. 1 della LBCR). Ai sensi dell'art. 2 cpv. 1 della LBCR, l'Ordinanza sulle banche estere-FINMA (OBE-FINMA) si applica per analogia anche agli istituti fintech.
- 24 Per «**soggetti stranieri** ai sensi dell'art. 1b LBCR» si intende quindi qualsiasi
7 impresa costituita secondo il diritto estero che possieda all'estero un'autorizzazione riconosciuta come equivalente all'autorizzazione fintech o che eserciti l'attività di una «persona ai sensi dell'art. 1b LBCR» (art. 1b cpv. 1 in combinato disposto con l'art. 2 LBCR e con l'art. 1 cpv. 1 ORB-FINMA).
- 24 Una «persona estera ai sensi dell'art. 1b LBCR» necessita di
8 un'**autorizzazione** della FINMA qualora impieghi in Svizzera persone che, per suo conto, concludono affari in modo continuativo e a titolo professionale in Svizzera o dalla Svizzera, gestiscono conti clienti o assumono impegni giuridici (cosiddetta succursale) oppure qualora operi in altro modo per conto delle «persone straniere ai sensi dell'art. 1b LBCR», in particolare trasmettendo loro ordini dei clienti o rappresentandole a fini pubblicitari o di altro tipo (cosiddetta rappresentanza) (art. 1b cpv. 1 in combinato disposto con l'art. 2 LBCR in combinato disposto con l'art. 2 cpv. 1 OAD-FINMA).

L'OAB-FINMA non è applicabile se la «persona straniera ai sensi dell'art. 1b LBCR» è effettivamente gestita dalla Svizzera o svolge la propria attività esclusivamente o prevalentemente in Svizzera o dalla Svizzera, poiché in tal caso si applicano gli **obblighi di autorizzazione ordinari** della LBCR (cfr. art. 1 cpv. 2 OAB-FINMA). 24
9

L'art. 19 cpv. 2 dell'Ordinanza sulle banche (OB) precisa che, in caso di istituzione di una **rappresentanza** permanente di una «persona estera ai sensi dell'art. 1b della LBCR», la reciprocità è garantita anche qualora le banche svizzere possano aprire rappresentanze permanenti con le stesse funzioni nello Stato estero. L'art. 19 cpv. 2 dell'Ordinanza sulle banche (OB) non richiede quindi che anche gli intermediari finanziari svizzeri possano aprire rappresentanze all'estero. Inoltre, il Consiglio federale è autorizzato, sulla base del riconoscimento reciproco di norme e misure di vigilanza equivalenti, a concludere trattati internazionali che prevedano che «le persone straniere ai sensi dell'art. 1b LBCR» provenienti dagli Stati contraenti possano aprire una succursale o una rappresentanza senza l'autorizzazione della FINMA (art. 1b cpv. 1 in combinato disposto con l'art. 2 cpv. 3 LBCR). Viceversa, la FINMA può assoggettare integralmente le «persone estere ai sensi dell'art. 1b LBCR» alle disposizioni applicabili agli istituti fintech nazionali, purché il diritto dello Stato in cui hanno sede le «persone estere ai sensi dell'art. 1b LBCR» non conceda agli istituti fintech svizzeri agevolazioni equivalenti e nessun trattato internazionale vi si opponga (cfr. art. 3 cpv. 2 OAV-FINMA). 25
0

In una prima fase si pone innanzitutto la questione di quali forme giuridiche estere corrispondano ai requisiti per l'autorizzazione fintech. Qualora venga riconosciuta una tale **equivalenza** e quindi l'obbligo di autorizzazione, in una seconda fase si pone la questione se sia possibile ottenere l'autorizzazione sia per una succursale che per una rappresentanza, in applicazione per analogia dell'OAB-FINMA. 25
1

VI. MODIFICHE ALL'AUTORIZZAZIONE

Gli istituti fintech devono comunicare alla FINMA ogni **modifica** dei fatti su cui si basa l'autorizzazione (art. 8a cpv. 1 OB) alla FINMA. Se le modifiche sono sostanziali, per il proseguimento dell'attività è necessario ottenere preventivamente un'autorizzazione della FINMA (art. 8a cpv. 2 OB). Modifiche sostanziali e di merito al modello di business durante la durata del 25
2

rapporto di vigilanza (ad es. modifica del modello di business) comportano, se del caso, la necessità di adeguare il regolamento interno e, eventualmente, lo statuto.

25 Nelle **linee guida della FINMA** relative all'autorizzazione nel settore fintech,
3 al punto II, viene elencato in modo non esaustivo ciò che si qualifica come modifica di rilevanza sostanziale ai sensi dell'art. 8a cpv. 2 OB e che richiede pertanto un'autorizzazione preventiva della FINMA. Sono comprese le seguenti modifiche:

- Modifica relativa ai documenti organizzativi (in particolare statuti e OGR; cfr. anche l'art. 10 lett. a dell'Ordinanza sugli istituti finanziari (OIF);
- modifiche relative ai soggetti qualificati (cfr. in dettaglio l'art. 10 lett. d ed e OIF);
- modifiche relative alle persone incaricate dell'amministrazione o della direzione (cfr. anche l'art. 10 lett. b OIF);
- modifiche relative all'organizzazione (ad es. modifiche al controllo dei rischi o alla funzione di compliance);
- se previsto: modifiche alla configurazione tecnica relative alla custodia di valori patrimoniali basati su criptovalute;
- modifiche relative alle norme interne in materia di governo societario (Corporate Governance);
- modifiche relative all'attività e ai servizi accessori (settore di attività);
- Modifiche relative all'esternalizzazione di servizi essenziali;
- Avvio, modifica o cessazione dell'attività all'estero (le società affiliate, le succursali e le rappresentanze devono sempre essere menzionate anche nel registro delle imprese);
- Fusione, scissione, trasformazione o trasferimento patrimoniale ai sensi della LFus del 3 ottobre 2003 (LFus); nonché
- cambio della società di revisione in Svizzera e all'estero.

25 La **domanda** di autorizzazione alla modifica deve contenere una motivazione
4 dettagliata (compresa l'analisi dei rischi). Tutte le informazioni rilevanti devono essere documentate e i documenti modificati devono essere allegati in una versione in cui siano evidenziate le modifiche. A seconda della natura

delle modifiche, si raccomanda di concordarle preventivamente con la FINMA.

VII. CRONOLOGIA DELLE AUTORIZZAZIONI

Finora la FINMA ha autorizzato **in totale 7 istituti fintech**: Bivial AG (ex 25 Klarpay AG), Relio AG, SR Saphirstein AG, Yapeal AG, Mogli AG, SWISS4.0 5 AG e Sequence SA. Attualmente, tuttavia, solo 5 di questi istituti fintech sono ancora operativi.

Con la SWISS4.0 AG, nel 2025, dopo la Mogli AG nel 2022, un altro istituto 25 fintech autorizzato ha dovuto essere nuovamente **liquidato**. Secondo le 6 informazioni pubbliche, la FINMA aveva sottoposto la SWISS4. 0 AG e aveva richiesto tempestivamente l'adozione di misure volte a migliorare la situazione finanziaria della start-up. La SWISS4.0 AG e i suoi organi non sono stati in grado di attuare con successo misure adeguate entro un termine ragionevole. Il 4 marzo 2025, a causa dei fondati timori di un indebitamento eccessivo e di gravi problemi di liquidità, la FINMA ha aperto la procedura di fallimento nei confronti della società fintech. La FINMA ha nominato Valfor Avocats Sàrl come liquidatore fallimentare. La SWISS4.0 AG era una cosiddetta micro con circa 250 clienti.

Anche nel 2024 la vigilanza sugli istituti titolari di un'autorizzazione ai sensi 25 dell'art. 1b LBCR si è rivelata intensa. In primo piano vi era la tutela dei 7 depositanti a causa della situazione di scarsità di capitale e di liquidità degli istituti. Gli istituti fintech sono di norma **start-up**, che, come prevedibile, sostengono spese elevate per la fase di avvio e l'ingresso sul mercato e che inizialmente non dispongono di ricavi o ne hanno solo di modesti. Un ingresso sul mercato di successo dipende dal buon esito dei round di finanziamento e da un modello di business sostenibile. Finora i modelli di business si collocano esclusivamente nel settore dei servizi di pagamento. Il mercato in questo settore è competitivo e i margini sono ridotti. È emerso che i modelli di business che si rivolgono a una nicchia con un'offerta unica o a un segmento di clientela specializzato possono avere successo.

Il mercato dei **servizi di pagamento** in Svizzera è molto competitivo ed 25 economicamente impegnativo. La cessazione dell'attività non è rara per le 8 start-up in un mercato così saturo. Ciò spiega anche perché quasi un terzo delle imprese autorizzate ai sensi dell'art. 1b della LBCR abbia cessato

l'attività. Inoltre, a differenza dei clienti bancari, i clienti degli istituti fintech non godono di alcuna tutela dei depositi. Non beneficiano nemmeno di alcun privilegio in caso di fallimento, sebbene i fondi dei clienti siano iscritti nel bilancio dell'istituto. Ciò comporta non solo maggiori rischi di insolvenza per i clienti e difficoltà a livello di vigilanza, ma anche, in un contesto altamente competitivo, una minore attrattiva di questa tipologia di autorizzazione.

- 25 La **FINMA**, soprattutto in questo contesto, richiede giustamente che gli
9 istituti fintech dispongano di una pianificazione continua del capitale e della liquidità e siano in grado di individuare tempestivamente eventuali difficoltà. Ciononostante, nel 2024 si sono verificate situazioni pericolose presso diversi istituti. La situazione si è spesso aggravata a causa della discutibile valore residuo delle attività in *scenari di crisi*, quando un'impresa aveva difficoltà a proseguire la propria attività e si doveva prendere in considerazione la liquidazione. Ciò riguardava in particolare la valutazione del software sviluppato internamente, che spesso rappresenta un'attività essenziale e che, sotto la pressione del tempo, a volte risulta difficile da cedere.

VIII. ULTERIORE SVILUPPO DELL'AUTORIZZAZIONE NEL SETTORE FINTECH

- 26 Nel suo rapporto «Digital Finance: ambiti d'intervento 2022+ », nell'ambito di
0 intervento 1, ha incaricato il DFF/SIF di riesaminare, in collaborazione con la FINMA e con il coinvolgimento del settore, l'attuale quadro giuridico e di vigilanza in relazione alle condizioni quadro per i nuovi operatori e le nuove forme di servizi.
- 26 La FINMA ha valutato in linea di principio positivamente l'autorizzazione
1 fintech nell'ambito di tale revisione. Tuttavia, ha indicato la mancanza di protezione dei fondi dei clienti in caso di fallimento come un grave svantaggio della normativa vigente. A causa di questa mancanza di protezione, vengono posti requisiti più elevati alla vigilanza, tanto più che gli istituti in questo settore non dispongono di una situazione reddituale stabile, soprattutto nella fase iniziale. È quindi indispensabile un monitoraggio tempestivo della situazione patrimoniale dell'istituto. L'onere di vigilanza della FINMA per gli istituti fintech è pertanto sproporzionato rispetto ad altri soggetti sottoposti a vigilanza. La FINMA ha inoltre individuato ulteriori carenze nell'attuale regolamentazione che rendono più difficile l'attività di vigilanza, in particolare

la possibilità di una revisione contabile limitata da parte della società di revisione (cfr. art. 1b cpv. 4 lett. b LBCR), i requisiti patrimoniali minimi o lo svolgimento di attività accessorie da parte degli istituti fintech.

In un'ottica di approccio globale, il Consiglio federale ritiene opportuno integrare la soluzione da esso perseguita nei relativi **lavori di regolamentazione**. La soluzione auspicata prevede in particolare una migliore tutela dei depositi del pubblico in caso di fallimento di un istituto di cui all'art. 1b. A tal fine, il Consiglio federale ritiene necessario un adeguamento della regolamentazione dei mercati finanziari volto a migliorare la protezione dei clienti. La mancanza di **protezione dei clienti** si riferisce solo ai depositi del pubblico raccolti, ma non alle attività basate su criptovalute (separabili) che possono essere raccolte nell'ambito di un'autorizzazione ai sensi dell'art. 1b LBCR. ²⁶

Nota

La presente pubblicazione riflette esclusivamente l'opinione personale degli autori e non vincola la FINMA.

Si ringrazia sentitamente il dott. Nico Hess per la revisione del manoscritto.

BIBLIOGRAFIA

Andreotti Fabio/Zimmermann Stephan/Prantl Florian, Custodial Staking, GesKR 3 (2023), S. 333-354.

Bahar Rashid/Stupp Eric, Kommentierung zu Art. 1 BankG, in: Watter Rolf/Vogt Nedim Peter/Bauer Thomas/Winzeler Christoph (Hrsg.), Basler Kommentar, Bankengesetz, 2. Aufl., Basel 2013.

Bertschinger Urs, Das Finanzmarktaufsichtsrecht vom vierten Quartal 2017 bis ins vierte Quartal 2018, SZW (2018), S. 708-725.

Bezzola(-Büchler) Dumeng N., Praktische Problemfelder und Lösungsansätze in Bezug auf die «FinTech»-Bewilligungsvoraussetzungen von Art. 1b BankG, SZW (2020), S. 534-556.

Bösch René, Kommentierung zu Art. 4^{quater} BankG, in: Watter Rolf/Vogt Nedim Peter/Bauer Thomas/Winzeler Christoph (Hrsg.), Basler Kommentar, Bankengesetz, 2. Aufl., Basel 2013.

Chapuis Cédric, Kommentierung zu Art. 2 BankG, in: Watter Rolf/Vogt Nedim Peter/Bauer Thomas/Winzeler Christoph (Hrsg.), Basler Kommentar, Bankengesetz, 2. Aufl., Basel 2013.

Chapuis Cédric, Kommentierung zu Art. 3^{bis-ter} BankG, in: Watter Rolf/Vogt Nedim Peter/Bauer Thomas/Winzeler Christoph (Hrsg.), Basler Kommentar, Bankengesetz, 2. Aufl., Basel 2013.

Chapuis Cédric, Kommentierung zu Art. 3^{quater} BankG, in: Watter Rolf/Vogt Nedim Peter/Bauer Thomas/Winzeler Christoph (Hrsg.), Basler Kommentar, Bankengesetz, 2. Aufl., Basel 2013.

Clemetson Caroline/Etienne Joane, Kommentierung zu Art. 6 FINIG, in: Sethe Rolf/Bösch René/Favre Olivier/Schott Ansgar (Hrsg.), Schulthess Kommentar, Finanzinstitutsgesetz, Zürich 2021.

Frick Thomas/Häusermann Marco, Kommentierung zu Art. 6 FINIG, in: Bahar Rashid/Watter Rolf (Hrsg.), Basler Kommentar Finanzdienstleistungsgesetz/Finanzinstitutsgesetz, 1. Aufl., Basel 2023.

Hess Nico, Geltungsbereich der bewilligungspflichtigen Tätigkeiten im Bankenrecht de lege lata und de lege ferenda, SSFM 142, Zürich 2023.

Hutzler Doris/Meirich David, Kommentierung zu Art. 2 Abs. 3 GwG, in: Graf Damian K/ Hutzler Doris (Hrsg.), Onlinekommentar zum Bundesgesetz über die Bekämpfung der Geldwäscherei und der Terrorismusfinanzierung – Version: 25.01.2026.

Maurenbrecher Benedikt/Kramer Stefan, Kommentierung zu Art. 3d BankG, in: Watter Rolf/Vogt Nedim Peter/Bauer Thomas/Winzeler Christoph (Hrsg.), Basler Kommentar, Bankengesetz, 2. Aufl., Basel 2013.

Meirich David, Regulatorische Einordnung von Decentralized Finance, SSFM 144, Zürich 2023.

Nobel Peter/Brändli Beat/Mächler Monika/Schiltknecht Florian, Schweizerisches Finanzmarktrecht, 5. Aufl., Bern 2026.-

Obrecht Matthias, Fintech-Bewilligung in der Schweiz, Netzwoche vom 10.06.2026, abrufbar unter: <https://www.netzwoche.ch/news/2026-06-10/fintech-bewilligung-in-der-schweiz-chancen-huerden-und-erfahrungen>, besucht am 12.06.2026 (zit. Obrecht, Netzwoche vom 10.6.2026).

Pfiffner Daniel C., Kommentierung zu Art. 24 FINMAG, in: Watter Rolf/Bahar Rashid (Hrsg.), Basler Kommentar, Finanzmarktaufsichtsgesetz/Finanzmarktinfrastrukturgesetz, 3. Aufl., Basel 2019.

Studer Ueli/Vollenweider Marino, Kommentierung zu Art. 43 FinfraG, in: Watter Rolf/Bahar Rashid (Hrsg.), Basler Kommentar, Finanzmarktaufsichtsgesetz/Finanzmarktinfrastrukturgesetz, 3. Aufl., Basel 2019.

Takei Yuto/Shudo Kazuyuki, Pragmatic Analysis of Key Management for Cryptocurrency Custodians, *IEEE International Conference on Blockchain and Cryptocurrency (ICBC)*, Dublin 2024, S. 747-765, abrufbar unter: <https://takeiyuto.github.io/assets/ckms.pdf> (besucht am 12.6.2026).

Winzeler Christoph, Kommentierung zu Art. 3 BankG, in: Watter Rolf/Vogt Nedim Peter/Bauer Thomas/Winzeler Christoph (Hrsg.), Basler Kommentar, Bankengesetz, 2. Aufl., Basel 2013.

I MATERIALI

Bericht des Bundesrates zu Anpassungen des Bankengesetzes vom 15. Juni 2018, abrufbar unter: <https://www.efd.admin.ch/dam/de/sd-web/hcvaF5Xv3zfo/aenderung-bankgesetz-bericht-de.pdf>, besucht am 27.4.2026 (zit. Bundesrat, Bericht Bankengesetz).

Bundesrat, Bericht Digital Finance: Handlungsfelder 2022+ vom 1. Februar 2022, abrufbar unter: <https://www.newsd.admin.ch/newsd/message/attachments/70095.pdf>, besucht am 25.4.2025 (zit. Bundesrat, Bericht Digital Finance).

Bundesrat, Bericht vom 16. Dezember 2022 zu Anpassungen des Bankengesetzes vom 15. Juni 2018, abrufbar unter: <https://backend.efd.admin.ch/fileservice/sdweb-docs-prod-efdadminch-files/files/2024/04/30/9fb7f508-2522-428c-a192-23b975c48e93.pdf>, besucht am 24.4.2025 (zit. Bundesrat, Bericht 2022).

EFD, Ergebnisbericht des Bundesrates zur Vernehmlassung zur Änderung der BankV FinTech-Bewilligung vom 21. Juni 2018, abrufbar unter: <https://www.newsd.admin.ch/newsd/message/attachments/52823.pdf>, besucht am 4.4.2025 (zit. EFD, Ergebnisbericht BankV FinTech-Bewilligung 2018).

EFD, Erläuterungsbericht DLT-Verordnung vom 18. Juni 2021, <https://www.newsd.admin.ch/newsd/message/attachments/67150.pdf>, besucht am 10.4.2025 (zit. EFD, Erläuterungsbericht DLT 2021).

EFD, Erläuterungsbericht DLT-Verordnung zur Vernehmlassungsvorlage vom 22. März 2019, abrufbar unter: <https://www.newsd.admin.ch/newsd/message/attachments/56192.pdf>, besucht am 10.4.2025 (zit. EFD, Erläuterungsbericht DLT-Verordnung).

EFD, Erläuterungsbericht Revision der Bankenverordnung (BankV) «FinTech-Bewilligung» vom 30. November 2018, abrufbar unter: <https://www.newsd.admin.ch/newsd/message/attachments/54881.pdf>, besucht am 4.4.2025 (zit. EFD, Erläuterungsbericht BankV 2018).

EFD, Erläuterungsbericht zur Änderung der Bankenverordnung (Fintech) vom 5. Juli 2017, abrufbar unter: <https://www.newsd.admin.ch/newsd/message/attachments/49033.pdf>, besucht am 4.4.2025 (zit. EFD, Erläuterungsbericht BankV 2017).

FINMA, Aufsichtsmitteilung 03/2024 - Erkenntnisse aus der Cyber-Risiko-Aufsichtstätigkeit, Präzisierung zur FINMA-Aufsichtsmitteilung 05/2020 und zu szenariobezogenen Cyber-Übungen, 7. Juni 2024, abrufbar unter: https://www.finma.ch/de/~media/finma/dokumente/dokumentencenter/myfinma/4dokumentation/finma-aufsichtsmitteilungen/20160707-finma-aufsichtsmitteilung-03-2024.pdf?sc_lang=de&hash=666EEE255C04FB42F01BFD0BC6C80191, besucht am 9.5.2025 (zit. FINMA, Aufsichtsmitteilung 03/2024).

FINMA, Aufsichtsmitteilung 03/2023 – Staking, 20. Dezember 2023, besucht am 23.4.2026, abrufbar unter https://www.finma.ch/de/~media/finma/dokumente/dokumentencenter/myfinma/4dokumentation/finma-aufsichtsmitteilungen/20231220-finma-aufsichtsmitteilung-08-2023.pdf?sc_lang=de&hash=19EEFFAA320ADED4258F199A8B5C6641 (zit. FINMA, Aufsichtsmitteilung 08/2023).

FINMA, Beurteilung von Bewilligungsprojekten und Vorfragen, abrufbar unter: <https://www.finma.ch/de/bewilligung/fintech/fintech-bewilligung/beurteilung-von-bewilligungsprojekten-und-vorfragen/>, besucht am 4.4.2025 (zit. FINMA, Beurteilung von Bewilligungsprojekten und Vorfragen).

FINMA, Erläuterungen zu Rundschreiben 2008/21 „Operationelle Risiken – Banken“ – Totalrevision und Rundschreiben 2013/3 „Prüfwesen“ – Teilrevision, 7. Dezember 2022, abrufbar unter: https://www.finma.ch/de/~media/finma/dokumente/dokumentencenter/anhoerungen/abgeschlossene-anhoerungen/20220510-op-risk-banken/20221213_rs_operat_risiken_anhoerung_eb.pdf?sc_lang=de&hash=050283AF582ECB06D725C6939DCAEC59, besucht am 9.5.2025 (zit. FINMA, Erläuterungen zu RS 2008/21).

FINMA, Fintech Start-up SWISS4.0 SA in Liquidation, Medienmitteilung vom 4. März 2025, abrufbar unter: https://www.finma.ch/de/news/2025/03/20250304-mm-fintech-startup-swiss4_0-liquidation/, besucht am 5.4.2025 (zit. FINMA, Fintech Start-up Swiss4.0 SA in Liquidation).

FINMA, Fintech-Bewilligung, abrufbar unter: <https://www.finma.ch/de/bewilligung/fintech/fintech-bewilligung/>, besucht am 4.4.2025 (FINMA, Fintech-Bewilligung).

FINMA, Jahresbericht 2018, abrufbar unter: https://www.finma.ch/~media/finma/dokumente/dokumentencenter/myfinma/finma-publikationen/geschaeftsbericht/20190404-finma-jahresbericht-2018.pdf?sc_lang=de&hash=AAD7EF04090DB3FB5BD0EAF92D8540E0, besucht am 20.4.2026 (zit. FINMA, Jahresbericht 2018).

FINMA, Jahresbericht 2021, abrufbar unter: https://www.finma.ch/~media/finma/dokumente/dokumentencenter/myfinma/finma-publikationen/geschaeftsbericht/20220405-finma_jahresbericht_2021.pdf, besucht am 10.4.2025 (zit. FINMA, Jahresbericht 2021).

FINMA, Jahresbericht 2024, abrufbar unter: https://www.finma.ch/de/~media/finma/dokumente/dokumentencenter/myfinma/finma-publikationen/geschaeftsbericht/20250408-finma_jb24.pdf?sc_lang=de&hash=F5BC9340E3211CAB036BEB2D7A71D2E0, besucht am 10.4.2025 (zit. FINMA, Jahresbericht 2024).

FINMA, Liste der von der FINMA bewilligten Personen nach Art. 1b BankG (Fintech-Bewilligung), abrufbar unter: <https://www.finma.ch/de/~media/finma/dokumente/bewilligungstraeger/pdf/fintech.pdf>, besucht am 5.4.2025 (zit. FINMA, Liste der von der FINMA bewilligten Personen nach Art. 1b BankG (Fintech-Bewilligung)).

FINMA, Neubewilligung von Banken und Wertpapierhäusern, abrufbar unter: <https://www.finma.ch/de/bewilligung/banken-und-wertpapierhaeuserh%C3%A4user/neubewilligung/>, besucht am 28.4.2025 (zit. FINMA, Neubewilligung von Banken und Wertpapierhäusern).

FINMA, Rundschreiben 2017/1, Corporate Governance - Banken, vom 22. September 2016, abrufbar unter: https://www.finma.ch/de/~media/finma/dokumente/rundschreiben-archiv/2017/rs-17-01/finma-rs-2017-01-20210506_de.pdf?sc_lang=de&hash=7F530363D0237EC203704EFC8E32C624, besucht am 4.4.2025 (zit. FINMA-RS 2017/1).

FINMA, Rundschreiben 2018/3, Outsourcing, vom 21. September 2017, abrufbar unter: https://www.finma.ch/de/~media/finma/dokumente/dokumentencenter/myfinma/rundschreiben/finma-rs-2018-03-01012021_de.pdf, besucht am 4.4.2025 (zit. FINMA-RS 2018/3).

FINMA, Rundschreiben 2023/01, «Operationelle Risiken und Resilienz – Banken», vom 7. Dezember 2022, abrufbar unter: <https://www.finma.ch/de/~media/finma/dokumente/dokumentencenter/myfinma/rundschreiben/finma-rs-2023-01-20221207.pdf>, besucht am 4.4.2025 (zit. FINMA-RS 2023/01).

FINMA, Rundschreiben 2025/4, «Konsolidierte Aufsicht von Finanzgruppen nach BankG und FINIG», vom 1. Juli 2025, abrufbar unter: https://www.finma.ch/de/~media/finma/dokumente/dokumentencenter/myfinma/rundschreiben/finma-rs-2025-04-20250305.pdf?sc_lang=de&hash=76CE12DBF3489A69BDE38B52875E081F, besucht am 4.4.2025 (zit. FINMA-RS 2025/4).

FINMA, Wegleitung für der FINMA einzureichende Bestätigungen der Prüfgesellschaften zu Gesuchen betreffend die Bewilligung als Personen nach Art. 1b BankG („Fintech-Unternehmen“) vom 10. April 2019, abrufbar unter: https://www.finma.ch/de/~media/finma/dokumente/dokumentencenter/myfinma/1bewilligung/fintech/w_institutsbewilligung-fintech_20190403_de.pdf?sc_lang=de&hash=0571D3925B8E6DA127785B8E1A8DC0BB, besucht am 4.4.2025 (zit. FINMA, Wegleitung für der FINMA einzureichende Bestätigungen der Prüfgesellschaften).

FINMA, Wegleitung für Gesuche betreffend Bewilligung als Person nach Art. 1b Bankengesetz (Fintech-Bewilligung) vom 24. April 2025, abrufbar unter: https://www.finma.ch/de/~media/finma/dokumente/dokumentencenter/myfinma/1bewilligung/fintech/w_bewilligungfintech_20250424.pdf?sc_lang=de&hash=DC7EB79EC1BDFD9E6C31C36306DAFA09, besucht am 4.4.2025 (zit. FINMA, Wegleitung Fintech-Bewilligung).