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

Circolare 2008/21
Rischi operativi – banche

Esigenze di fondi propri ed esigenze qualitative per i rischi operativi nel settore bancario

Riferimento:	Circ. FINMA 08/21 «Rischi operativi – banche»
Data:	20 novembre 2008
Entrata in vigore:	1° gennaio 2009
Ultima modifica:	31 ottobre 2019 [le modifiche sono contrassegnate con un * ed elencate alla fine del documento]
Concordanza:	sostituisce la Circ. CFB 06/3 «Rischi operativi» del 29 settembre 2006
Basi legali:	LFINMA art. 7 cpv. 1 lett. b
	LBCR art. 3 cpv. 2 lett. a e b, 3*g*, 4 cpv. 2 e 4, 4bis cpv. 2
	OBCR art.12
	LBVM art. 10 cpv. 2 lett. a
	OBVM art. 19 cpv. 3, 20 cpv. 1, 29
	OFoP art. 2, 89-94
	Oem-FINMA art. 5 e segg.
Allegato 1:	Classificazione degli ambiti di attività conformemente all'art. 93 cpv. 2 OFoP
Allegato 2:	Panoramica della categorizzazione dei tipi di eventi
Allegato 3:	Trattamento dei dati elettronici dei clienti

Destinatari																													
LBCR			LSA			LBVM	LInFi						LICol										LRD			Altri			
Banche	Gruppi e congl. finanziari	Altri intermediari	Assicuratori	Gruppi e congl. assicurativi	Intermediari assicurativi	Commercianti di val. mobiliari	Sedi di negoziazione	Controparti centrali	Depositari centrali	Repertori di dati sulle negoziazioni	Sistemi di pagamento	Partecipanti	Direzioni dei fondi	SICAV	Società in accomandita per ICC	SICAF	Banche depositarie	Gestori patrimoniali di ICC	Distributori	Rappresentanti di ICC esteri	Altri intermediari	OAD	IFDS	Assoggettati OAD	Società di audit	Agenzie di rating		
X	X					X																							

Laupenstrasse 27, 3003 Berna
Tel. +41 (0)31 327 9100, fax +41 (0)31 327 9101
www.finma.ch

Indice

Indice

I. Oggetto

La presente circolare concretizza gli art. 89-94 dell'Ordinanza sui fondi propri (OFoP; RS 952.03) e disciplina le esigenze qualitative di base per la gestione dei rischi operativi ai sensi dell'art. 12 OBVM e degli art. 19–20 OBVM. Nell'ambito quantitativo disciplina le esigenze di fondi propri per i rischi operativi in base ai tre approcci disponibili e gli obblighi che ne derivano. Le esigenze qualitative di base corrispondono alle raccomandazioni del Comitato di Basilea per la vigilanza bancaria sulla gestione irreprensibile dei rischi operativi. 1*

II. Definizione

L'art. 89 OFoP definisce i rischi operativi come «il pericolo di perdite consecutive all'inadeguatezza o all'inefficacia delle procedure interne, delle persone o dei sistemi oppure dovute a eventi esterni». La definizione comprende tutti i rischi legali e di *compliance*, purché rappresentino una perdita finanziaria diretta, cioè inclusi le multe inflitte dalle autorità di vigilanza e gli accordi transattivi. 2*

Abrogato 2.1*

III. Esigenze di fondi propri

A. Approccio dell'indicatore di base (BIA, art. 92 OFoP)

Per le banche che si avvalgono dell'approccio dell'indicatore di base (*basic indicator approach*, BIA) per calcolare le esigenze di fondi propri per i rischi operativi, tali esigenze equivalgono al prodotto del moltiplicatore α per la media dei tre anni precedenti degli indicatori annuali di ricavo GI[1]. Ai fini del calcolo della media si considerano tuttavia soltanto gli anni nei quali il GI ha un valore positivo. 3

I tre anni precedenti di cui al nm. 3 (e al nm. 24) corrispondono ai tre periodi annuali che precedono direttamente la data di allestimento dell'ultimo conto economico pubblicato. Per esempio, se l'ultimo conto economico è stato pubblicato in data 30 giugno 2008, i tre anni da prendere in considerazione corrispondono agli esercizi dal 1° luglio 2005 al 30 giugno 2006, dal 1° luglio 2006 al 30 giugno 2007 e dal 1° luglio 2007 al 30 giugno 2008. 4

Le esigenze di fondi propri K_{BIA} sono calcolate quindi con la seguente formula: 5

$$K_{BIA} = \alpha \cdot \sum_{j=1}^{3} \frac{\max[0,\ GI_j]}{\max[1,\ n]}$$

Dove

- α è fissato uniformemente al 15%; 6

[1] Nella versione rivista degli standard minimi del Comitato di Basilea sulla vigilanza bancaria (*International Convergence of Capital Measurement and Capital Standards – A Revised Framework / Comprehensive Version*) del giugno 2006 l'indicatore di ricavo è denominato *gross income* (GI).

- GI_j corrisponde all'indicatore di ricavo dell'anno j; e 7

- n rappresenta il numero di anni, tra i tre precedenti, in cui è stato registrato un indicatore di ricavo GI positivo. 8

L'indicatore di ricavo GI corrisponde alla somma delle seguenti posizioni del conto economico secondo il nm. 125 e segg. della Circ. FINMA 15/1 «Direttive contabili – banche»: 9*

- risultato lordo da operazioni su interessi (nm. 131 Circ. FINMA 15/1 «Direttive contabili – banche»); 10*

- risultato da operazioni in commissione e da prestazioni di servizio[2] (nm. 139 Circ. FINMA 15/1 «Direttive contabili – banche»); 11*

- risultato da attività di negoziazione e dall'opzione "fair value" (nm. 140 Circ. FINMA 15/1 «Direttive contabili – banche»); 12*

- proventi da partecipazioni non consolidate (nm. 143 Circ. FINMA 15/1 «Direttive contabili – banche»); e 13*

- risultato da immobili (nm. 144 Circ. FINMA 15/1 «Direttive contabili – banche»). 14*

La base per la determinazione dell'indicatore di ricavo GI a livello consolidato corrisponde all'area di consolidamento adottata per calcolare le esigenze di fondi propri. 15

In caso di ampliamento della struttura o delle attività di una banca (p. es. in seguito al rilevamento di una nuova unità operativa), occorre adeguare di conseguenza verso l'alto i valori storici dell'indicatore di ricavo GI. Le eventuali riduzioni dell'indicatore di ricavo GI (p. es. in seguito all'alienazione di una divisione) sono subordinate all'autorizzazione della FINMA. 16

Per determinare l'indicatore di ricavo GI ai sensi dell'art. 91 cpv. 1 OFoP, le banche possono applicare standard di rendiconto riconosciuti a livello internazionale anziché le prescrizioni svizzere sulla presentazione dei conti, a condizione che la FINMA conceda l'apposita autorizzazione (cfr. art. 91 cpv. 4 OFoP). 17

Tutti i ricavi provenienti da convenzioni di subfornitura (*outsourcing*) in cui la banca stessa figura come fornitore di servizi devono essere considerati parte integrante dell'indicatore di ricavo GI (cfr. art. 91 cpv. 2 OFoP). 18

Se la banca svolge il ruolo di subcommittente di una prestazione di servizi esternalizzata, le spese corrispondenti possono essere dedotte dall'indicatore di ricavo GI soltanto se la subfornitura è effettuata e registrata su base consolidata all'interno del medesimo gruppo finanziario (cfr. art. 91 cpv. 3 OFoP). 19

[2] La considerazione degli oneri per commissioni di cui al nm.138 della Circ. FINMA 15/1 «Direttive contabili – banche» è soggetta alle restrizioni di cui al nm. 18.

Abrogato 20*-22*

B. Approccio standard (SA, art. 93 OFoP)

a) Meccanismo

Per determinare le esigenze di fondi propri, le banche devono suddividere l'insieme delle loro attività nei seguenti ambiti: 23

i	**Ambito di attività**	β_i
1	Finanziamento / Consulenza d'imprese	18%
2	Negoziazione	18%
3	Attività bancaria al dettaglio per i privati	12%
4	Attività bancaria al dettaglio per le ditte	15%
5	Traffico dei pagamenti / Regolamento dei titoli	18%
6	Attività di deposito e depositi fiduciari	15%
7	Gestione patrimoniale istituzionale	12%
8	Attività di commissione su titoli	12%

Tabella 1

Per ogni ambito di attività i e per ciascuno dei tre anni precedenti di cui al nm. 4 viene calcolato un indicatore di ricavo in base ai nm. 9-18, poi moltiplicato per il corrispondente fattore β_i indicato nella tabella 1. I valori così ottenuti vengono sommati per ogni anno, fermo restando che eventuali valori negativi di taluni ambiti di attività possono essere compensati con valori positivi di altri ambiti di attività. Le esigenze di fondi propri corrispondono alla media triennale. In questo caso, per il calcolo della media, gli eventuali addendi negativi devono essere parificati a zero (cfr. art. 93 cpv. 1 OFoP). 24

Con l'approccio standard le esigenze di fondi propri K_{SA} si calcolano secondo la seguente formula: 25

$$K_{SA} = \frac{1}{3} \cdot \sum_{j=1}^{3} \max\left[0,\ \sum_{i=1}^{8} GI_{i,j} \cdot \beta_i\right]$$

dove

- $GI_{i,j}$ corrisponde all'indicatore di ricavo GI per l'ambito di attività i nell'anno j; e 26
- β_i corrisponde a una percentuale fissa per l'ambito di attività i, identica per tutte le banche. 27

b) Esigenze generali (art. 93 cpv. 3 OFoP)

Abrogato 28*

In conformità all'allegato 1, ogni banca deve definire principi specifici di ripartizione delle proprie attività negli ambiti di attività standardizzati di cui al nm. 23 e documentare 29*

opportunamente i criteri a tal proposito. Tali criteri devono essere periodicamente verificati e adeguati in funzione dei cambiamenti a livello di attività della banca.

c) Abrogato

Abrogato 30*-44*

C. Approcci specifici agli istituti (AMA, art. 94 OFoP)

a) Autorizzazione

Gli approcci specifici agli istituti (*advanced measurement approaches*, AMA) consentono alle banche di adottare una propria procedura per quantificare autonomamente, nel rispetto di determinati requisiti, le esigenze di fondi propri per i rischi operativi. 45

L'utilizzo di un approccio specifico all'istituto richiede un'apposita autorizzazione della FINMA. 46

Prima di concedere l'autorizzazione per l'utilizzo di un approccio specifico all'istituto, la FINMA può esigere che le banche eseguano, su un periodo massimo di due anni, calcoli fondati sull'approccio in questione, ai fini di test e di confronto. 47

Se una banca applica un approccio specifico all'istituto, può passare interamente o parzialmente all'approccio dell'indicatore di base o all'approccio standard unicamente su ingiunzione o previa autorizzazione della FINMA. 48

Le spese sostenute dalla FINMA per la procedura di autorizzazione e le necessarie verifiche successive al rilascio dell'autorizzazione vengono fatturate alle banche interessate. 49

b) Esigenze qualitative supplementari

Le banche che utilizzano un approccio specifico all'istituto devono soddisfare le esigenze qualitative di base di cui al capitolo IV.B. 50*

L'utilizzo di un approccio specifico all'istituto per il calcolo delle esigenze di fondi propri per i rischi operativi presuppone l'adempimento delle ulteriori esigenze qualitative elencate qui di seguito. 51

L'organo preposto all'alta direzione, alla vigilanza e al controllo deve essere coinvolto attivamente nel monitoraggio dell'approccio. 52

La direzione generale deve avere dimestichezza con il concetto alla base dell'approccio ed essere in grado di assolvere le sue funzioni di sorveglianza. 53*

Per la gestione dei rischi operativi, la banca deve disporre di un sistema concettualmente solido, affidabile e implementato nella sua integralità. 54

La banca deve disporre, a tutti i livelli, di risorse sufficienti per la gestione, il controllo e la revisione interna in relazione all'approccio specifico all'istituto. 55

La banca deve disporre di un'unità centrale indipendente per la gestione dei rischi operativi, che sia responsabile dell'elaborazione e dell'implementazione dei principi di gestione dei rischi operativi. Tale unità è competente per: 56

- la definizione di principi e procedure per la gestione e il controllo dei rischi operativi, validi per l'intera banca; 57
- l'elaborazione e l'implementazione di una metodologia di quantificazione dei rischi operativi propria dell'istituto; 58
- l'elaborazione e l'implementazione di un sistema di notifica dei rischi operativi; e 59
- lo sviluppo di strategie per l'individuazione, la misurazione, la sorveglianza e il controllo o la riduzione dei rischi operativi. 60

Il modello di quantificazione specifico all'istituto deve essere strettamente integrato nel processo di gestione quotidiana dei rischi della banca. 61

I risultati del modello di quantificazione specifico all'istituto devono costituire parte integrante delle procedure di sorveglianza e controllo del profilo di rischio. Queste informazioni devono, per esempio, essere poste in primo piano nella stesura dei rapporti per la gestione, nell'allocazione interna dei fondi propri e nell'analisi dei rischi. 62

La banca deve disporre di metodi per l'allocazione dei fondi propri per i rischi operativi agli ambiti di attività importanti e per la creazione di sistemi di incentivi tesi a contribuire al miglioramento della gestione dei rischi operativi nell'intera banca. 63

Abrogato 64*

La revisione interna e la società di audit devono sottoporre a verifiche periodiche i processi di gestione dei rischi operativi e l'attuazione dell'approccio specifico all'istituto, comprendendo sia le attività delle singole unità operative sia quelle dell'unità centrale per la gestione dei rischi operativi. 65

La convalida del sistema di quantificazione da parte della società di audit deve contenere in modo particolare i seguenti elementi: 66

- verifica del buon funzionamento dei processi interni di convalida; e 67
- garanzia della trasparenza e dell'accessibilità dei flussi di dati e dei processi dell'approccio specifico all'istituto, assicurando in particolare che la revisione interna, la società di audit e la FINMA possano accedere alle specifiche e ai parametri dell'approccio. 68

c) Esigenze quantitative generali

In conformità agli standard minimi di Basilea[3], la FINMA non indica alcun approccio preciso, lasciando alle banche ampio spazio di manovra in materia. Pertanto, la presente circolare si limita a illustrare le esigenze essenziali da soddisfare obbligatoriamente ai fini dell'applicazione di detto approccio. L'esame delle peculiarità dettagliate di un approccio specifico all'istituto costituisce oggetto del processo di autorizzazione individuale, condotto dalla FINMA con il coinvolgimento della società di audit. 69

Indipendentemente dalla struttura concreta del suo approccio, la banca deve poter dimostrare che lo stesso tiene conto anche di eventi scarsamente probabili, ma in grado di generare perdite quantitativamente significative. Le esigenze di fondi propri risultanti dal modello adottato devono corrispondere approssimativamente al quantile 99,9% della funzione di distribuzione delle perdite operative aggregate sull'arco di un anno. 70

Ciascun approccio specifico all'istituto deve essere fondato su un concetto di rischio operativo compatibile con la definizione di cui all'art. 89 OFoP e al nm. 2 e consentire inoltre di classificare gli eventi che generano perdite conformemente all'allegato 2. 71*

I fondi propri necessari sono determinati sia per le perdite attese sia per quelle inattese. La FINMA può tuttavia concedere delle facilitazioni al riguardo, qualora la banca abbia costituito opportuni accantonamenti per le future perdite attese. 72

Tutte le ipotesi, esplicite e implicite, concernenti le interdipendenze tra gli eventi che generano perdite operative come pure tra le funzioni di stima utilizzate, devono essere plausibili e motivate. 73

Ogni approccio deve presentare determinate caratteristiche di base. Tra queste rientra, in particolare, l'adempimento dei requisiti relativi all'integrazione di: 74

- dati interni di perdita (nm. 76-85);
- dati esterni di perdita rilevanti (nm. 86-88);
- procedure di analisi degli scenari (nm. 89-91); e
- fattori legati al contesto di attività e al sistema interno di controllo (nm. 92-97).

Per l'integrazione di questi quattro fattori di input nell'approccio e per la determinazione della loro importanza relativa, la banca deve disporre di un concetto affidabile e trasparente, documentato in modo esauriente e verificabile. L'approccio deve essere coerente sul piano interno ed evitare, in particolare, che elementi tesi a ridurre il rischio (p. es. fattori legati al contesto operativo e al sistema interno di controllo o contratti di assicurazione) siano presi in considerazione più volte. 75

[3] Cfr. nota 1.

d) Dati interni di perdita (art. 94 cpv. 2 OFoP)

Una banca deve disporre di documentate procedure di valutazione della rilevanza continua nel tempo dei dati storici di perdita, comprendenti in particolare chiare regole interne concernenti le modalità di modifica dei dati relativi alle perdite (p. es. nessuna presa in considerazione per mancanza di attuale rilevanza, graduazione in funzione della variazione delle dimensioni o qualsiasi altra forma di aggiustamento), che definiscano inoltre chi è autorizzato a procedere a tali modifiche e in quale misura. 76

Una banca deve utilizzare una banca dati contenente i dati interni di perdita. Questa deve comprendere, al primo utilizzo dell'approccio a fini regolamentari, un periodo di osservazione di almeno tre anni. Al più tardi due anni dopo il primo utilizzo dell'approccio, tale periodo di osservazione viene esteso in modo duraturo ad almeno cinque anni. 77

Il processo di creazione di una banca dati interna per le perdite operative deve soddisfare le condizioni elencate qui di seguito: 78

- Al fine di agevolare la convalida regolamentare, la banca deve essere in grado di ripartire l'insieme dei dati interni di perdita tra gli ambiti di attività indicati al nm. 23 e tra i tipi di eventi elencati nell'allegato 2. Ai fini della ripartizione deve applicare criteri oggettivi e documentati. 79*

- Tutti i dati interni di perdita della banca devono essere raccolti attraverso un processo solido e integro. Tali dati devono riguardare tutte le attività ed esposizioni materiali, compresi tutti i sottosistemi e le localizzazioni geografiche rilevanti. Nella raccolta dei dati di perdita è consentito omettere la registrazione sistematica di perdite inferiori a un importo minimo lordo fissato dalla FINMA. 80

- Per ogni evento che genera una perdita, la banca deve raccogliere le seguenti informazioni: importo lordo della perdita, data dell'evento che l'ha causata ed eventuali attenuazioni della perdita (p. es. in seguito a contratti di assicurazione). Per gli eventi che generano perdite di importo lordo di almeno franchi svizzeri 1 milione, occorre descrivere le cause di tale evento. 81

- La banca deve definire i principi per la registrazione degli eventi che generano una perdita, comprendenti anche i criteri per la classificazione degli eventi che generano perdite all'interno di funzioni centrali (p. es. servizio informatico) o che interessano più ambiti di attività. Inoltre, deve essere disciplinata la modalità di trattamento di serie di eventi che generano perdite non indipendenti tra di loro. 82

Ai fini del calcolo delle esigenze di fondi propri, le perdite dovute a rischi operativi, sopraggiunte in rapporto ai rischi di credito e storicamente registrate dalla banca come rischio di credito, possono continuare a essere considerate esclusivamente come eventi associati al rischio di credito. Tuttavia, a partire da un determinato importo lordo fissato dalla FINMA, tali perdite devono essere integrate nella banca dati interna relativa alle perdite risultanti da rischi operativi e prese in considerazione per la gestione di questi ultimi. Tali eventi vanno registrati 83

in modo analogo agli altri dati interni di perdita, ma devono essere contrassegnati come non pertinenti ai fini del calcolo dei fondi propri per i rischi operativi.

Qualora una perdita dovuta a un rischio operativo si manifesti anche sotto forma di perdita legata al rischio di mercato, l'evento corrispondente deve essere registrato in modo analogo agli altri eventi di perdita e integrato nell'approccio specifico all'istituto. Se per calcolare le esigenze di fondi propri per i rischi di mercato una banca utilizza un modello di aggregazione dei rischi secondo i nm. 228-365 della Circ. FINMA 08/20 «Rischi di mercato – banche», le posizioni conseguenti a eventi legati ai rischi operativi non possono essere escluse dal calcolo del *value at risk*, del *value at risk* basato su uno scenario di stress, dell'*incremental risk charge*, della *comprehensive risk measure*, né dal *backtesting*. 84*

Nell'approccio specifico all'istituto, le eventuali perdite negative (p. es. utili su una posizione azionaria acquisita erroneamente) non possono sortire un effetto di riduzione dei fondi propri necessari. 85

e) Dati esterni di perdita (art. 94 cpv. 2 OFoP)

Le banche devono integrare nel loro approccio specifico gli eventuali dati esterni di perdita rilevanti, al fine di assicurare che si tenga conto anche di eventi rari ma potenzialmente gravi. Possono fungere da fonte di informazione pertinente i dati esterni di perdita pubblicamente accessibili, come pure quelli scambiati fra determinate banche. 86

In questi dati esterni di perdita si considera l'entità effettiva della perdita, informazioni concernenti l'estensione delle attività svolte dalla linea operativa interessata dalla perdita, le cause e le circostanze della perdita nonché delle informazioni concernenti la valutazione della portata dell'evento di perdita per la banca stessa. 87

Per l'utilizzo dei dati esterni di perdita, le banche devono definire e documentare un processo sistematico, comprendente in particolare una chiara metodologia di integrazione di questi dati nell'approccio specifico all'istituto (p. es. graduazione, adeguamenti qualitativi o effetti sull'analisi degli scenari). Le condizioni quadro e le procedure di utilizzo dei dati esterni di perdita devono essere sottoposte a verifiche periodiche interne e a verifiche da parte della società di audit. 88

f) Analisi di scenari (art. 94 cpv. 2 OFoP)

Gli approcci specifici all'istituto devono prendere in considerazione i risultati delle procedure di analisi degli scenari. 89

Le analisi degli scenari, basate sulle opinioni di esperti e su dati esterni, valutano il pericolo gravante sulla banca che si verifichino eventi di perdita potenzialmente gravi. 90

L'attualità e la pertinenza degli scenari utilizzati per l'analisi come pure i parametri ad essi attribuiti devono essere verificati e all'occorrenza adeguati in presenza di sostanziali variazioni della situazione di rischio, comunque almeno una volta all'anno. In caso di sostanziali variazioni della situazione di rischio, gli adeguamenti devono essere effettuati immediatamente. 91

g) Contesto di attività e sistema interno di controllo (art. 94 cpv. 2 OFoP)

A titolo prospettico, la banca deve inserire nell'approccio specifico degli indicatori previsionali tratti dal contesto nel quale esercita la sua attività e dal suo sistema interno di controllo. Tali indicatori hanno l'obiettivo di tenere conto specificatamente delle caratteristiche aggiornate del profilo di rischio della banca (p. es. nuove attività, nuove soluzioni informatiche, procedure modificate) o dei cambiamenti intervenuti nell'inquadramento generale (p. es. situazione della politica di sicurezza, modifica della giurisprudenza, minaccia di virus informatici). 92

Per poter essere utilizzati nell'ambito di un approccio specifico all'istituto, i fattori relativi al contesto operativo e al sistema interno di controllo devono soddisfare le condizioni elencate qui di seguito: 93

- Ogni fattore deve costituire un generatore di rischio rilevante alla luce delle esperienze maturate e della valutazione del segmento d'affari interessato. Il fattore deve essere idealmente quantificabile e controllabile. 94

- La sensibilità delle stime di rischio di una banca alle variazioni dei fattori e alla loro importanza relativa deve poter essere motivata e verificata. Oltre alle possibili variazioni del profilo di rischio legate a miglioramenti dell'ambiente di controllo, la strategia deve registrare in particolare anche i potenziali aumenti dei rischi dovuti a una maggiore complessità o alla crescita delle attività. 95

- La strategia in sé, nonché la scelta e l'applicazione dei singoli fattori, compresi i principi fondamentali dell'adeguamento delle stime empiriche, devono essere documentati. La documentazione deve inoltre essere sottoposta a verifica indipendente all'interno della banca. 96

- I processi, i relativi risultati e gli adeguamenti apportati devono essere confrontati a scadenze regolari con le perdite effettive rilevate empiricamente all'interno e all'esterno dell'istituto. 97

h) Riduzione del rischio tramite assicurazioni

Qualora utilizzino un approccio specifico all'istituto, nel calcolo delle esigenze di fondi propri per i rischi operativi le banche possono tenere conto dell'effetto di riduzione del rischio prodotto dai contratti di assicurazione. Tuttavia, il riconoscimento di tali effetti di copertura è limitato a un massimo del 20% delle esigenze di fondi propri, calcolate sulla base di un approccio specifico all'istituto. 98

Le possibilità di riduzione delle esigenze di fondi propri sono subordinate all'adempimento delle condizioni descritte qui di seguito: 99

- L'assicuratore deve beneficiare di un rating di credito a lungo termine pari o superiore alla classe 3, emesso da un'agenzia di rating riconosciuta dalla FINMA. 100

- Il contratto di assicurazione deve avere una durata iniziale minima di un anno. Qualora la durata residua sia inferiore a un anno, il riconoscimento dell'effetto di copertura deve 101

essere ridotto in modo lineare dal 100% (per una durata residua di almeno 365 giorni) fino allo 0% (per una durata residua di 90 giorni). Gli effetti di copertura derivanti dai contratti di assicurazione con una durata residua di 90 giorni o inferiore non sono riconosciuti nel calcolo delle esigenze di fondi propri.

- Il contratto di assicurazione deve prevedere un termine di disdetta di almeno 90 giorni. Se il termine di disdetta è inferiore a un anno, il riconoscimento dell'effetto di copertura si riduce in modo lineare dal 100% (per un termine di disdetta di almeno 365 giorni) fino allo 0% (per un termine di disdetta di 90 giorni). Tali percentuali si applicano anche agli effetti di copertura eventualmente già ridotti secondo il nm. 101. 102

- Il contratto di assicurazione non deve contenere alcuna clausola restrittiva o di esclusione che, in caso di intervento regolamentativo oppure di insolvibilità della banca in questione, possa estromettere la banca, il suo eventuale acquirente, la persona incaricata del risanamento o il liquidatore dalla corresponsione delle prestazioni assicurative. Tali clausole restrittive o di esclusione sono invece ammesse se si limitano esclusivamente agli eventi verificatisi dopo l'apertura della procedura fallimentare o della liquidazione. 103

- Il calcolo dell'effetto di copertura risultante dai contratti di assicurazione deve essere trasparente e coerente con le probabilità assunte dal metodo avanzato di misurazione e con le dimensioni di un potenziale evento di perdita. 104

- L'assicuratore deve essere un istituto esterno non appartenente allo stesso gruppo della banca. In caso contrario, gli effetti di copertura risultanti dai contratti di assicurazione saranno riconosciuti soltanto se l'assicuratore trasferisce a sua volta i rischi a una terza parte indipendente (p. es. una compagnia di riassicurazione). Ai fini del riconoscimento dell'effetto di copertura, questa terza parte indipendente deve soddisfare tutti i requisiti posti a un assicuratore. 105

- La strategia interna della banca riguardante le soluzioni assicurative deve essere orientata al trasferimento effettivo del rischio e documentata in modo esauriente. 106

- La banca deve pubblicare le informazioni che riguardano il ricorso a soluzioni assicurative volte a ridurre i rischi operativi. 107

D. Utilizzo parziale degli approcci

In linea di principio è consentito limitare l'utilizzo di un approccio specifico all'istituto a determinati settori di attività e applicare agli altri settori l'approccio dell'indicatore di base o l'approccio standard. A questo scopo, è richiesto l'adempimento delle condizioni elencate qui di seguito. 108

- Tutti i rischi operativi della banca devono essere registrati mediante uno dei metodi menzionati nella presente circolare, fermo restando che i relativi ambiti di attività devono soddisfare i requisiti stabiliti per il rispettivo approccio. 109

- Al momento dell'utilizzo di un approccio specifico all'istituto, esso deve comprendere una parte sostanziale dei rischi operativi della banca. 110

- La banca deve disporre di uno scadenzario in cui è riportata la tempistica dell'estensione dell'approccio specifico all'istituto a tutte le entità giuridiche e a tutti gli ambiti di attività materiali dell'istituto. 111

- Non è consentito mantenere il l'approccio dell'indicatore di base o l'approccio standard in determinati ambiti di attività al fine di minimizzare le esigenze di fondi propri. 112

La delimitazione tra l'approccio specifico all'istituto e l'approccio dell'indicatore di base o l'approccio standard può essere basata sugli ambiti di attività, sulle strutture giuridiche, sulle aree geografiche o su altri criteri distintivi chiaramente definiti a livello interno. 113

Tranne nei casi menzionati ai nm. 108-113, non è consentito calcolare le esigenze di fondi propri per i rischi operativi in una banca servendosi di metodi diversi. 114

E. Adeguamenti delle esigenze di fondi propri (art. 45 OFoP)

Nel quadro delle sue funzioni di vigilanza per quanto riguarda i fondi propri supplementari (art. 45 OFoP), la FINMA può aumentare individualmente le esigenze di fondi propri delle singole banche. Tali interventi si impongono, in particolare, quando un calcolo delle esigenze di fondi propri fondato esclusivamente sull'approccio dell'indicatore di base o sull' approccio standard comporterebbe esigenze di fondi propri inadeguatamente ridotte a causa di indicatori di ricavo GI troppo bassi. 115

F. Fondi propri minimi e limite inferiore (*floor*)

In applicazione della continuazione della soglia minima di patrimonio (*floor regime*) pubblicata dal Comitato di Basilea per la vigilanza bancaria vale il seguente principio[4]: per le banche che calcolano i propri rischi operativi in base al principio AMA, le esigenze minime in materia di fondi propri a livello della banca nel suo complesso, considerando anche le deduzioni di fondi propri computabili, non possono essere inferiori all'80% delle esigenze e delle deduzioni previste teoricamente per la banca secondo lo standard minimo di Basilea I[5]. In applicazione dell'art. 47 OFoP, nel caso di alcuni istituti specifici, la FINMA stabilisce come procedere al calcolo approssimativo adeguato delle esigenze teoriche secondo Basilea I. Per i rischi operativi si orienta all'approccio standard in conformità all'art. 93 OFoP 116*

[4] V. Comunicato stampa del Comitato di Basilea per la vigilanza bancaria del 13 luglio 2009: www.bis.org/press/p090713.htm (in inglese)

[5] Ciò corrisponderebbe al calcolo delle esigenze di fondi propri in conformità all'Ordinanza del 17 maggio 1972 sulle banche e le casse di risparmio in vigore fino al 31.12.2006 (RU **1995** 253, RU **1998** 16).

IV. Esigenze qualitative poste alla gestione dei rischi operativi

A. Principio di proporzionalità

Le esigenze sancite dal presente capitolo si applicano, in linea di principio, a tutti i destinatari della presente circolare. Dette esigenze dipendono tuttavia, nel singolo caso, dalle dimensioni, dalla complessità, dalla struttura e dal profilo di rischio dell'istituto. Il nm. 119 elenca i numeri marginali dalla cui applicazione sono interamente esclusi gli istituti di piccole dimensioni. 117*

Sono considerati istituti di piccole dimensioni ai sensi del nm. 117 le banche e i commercianti di valori mobiliari delle categorie FINMA[6] 4 e 5. Nel singolo caso, la FINMA può ordinare facilitazioni o inasprimenti. 118*

B. Esigenze qualitative di base

Gli istituti di piccole dimensioni conformemente ai nm. 117 e 118 sono esonerati dall'adempimento dei nm. 129 e 132-134. 119*

Le esigenze qualitative di base si basano sui «Principles for the Sound Management of Operational Risk» del Comitato di Basilea per la vigilanza bancaria (giugno 2011).[7] 120*

a) Principio 1: Categorizzazione e classificazione dei rischi operativi

I rischi operativi devono essere ripartiti in maniera unitaria in categorie, allo scopo di garantire la coerenza nel quadro dell'identificazione del rischio, della valutazione del rischio e della definizione degli obiettivi nella gestione operativa dei rischi[8]. 121*

La classificazione unitaria dei rischi operativi avviene sulla base della categorizzazione dei rischi operativi in conformità al nm. 121* e comprende una valutazione sia dei rischi inerenti[9] sia dei rischi residui[10]. La classificazione può essere effettuata sulla base di una valutazione sia qualitativa sia quantitativa. La classificazione serve in particolare anche a determinare i rischi di considerevole portata in conformità al nm. 137. 122*

Abrogato 123*-124*

b) Abrogato

Abrogato 125*-127*

[6] Cfr. l'Appendice della Circ. FINMA 11/2 «Margine di fondi propri e pianificazione del capitale – banche».
[7] www.bis.org/publ/bcbs195.pdf (in inglese)
[8] La categorizzazione unitaria può essere effettuata in conformità all'Allegato 2 della presente circolare oppure mediante una terminologia o una tassonomia interna.
[9] Cfr. Allegato 3, nm. 59
[10] Cfr. Allegato 3, nm. 60

c) Principio 2: identificazione, limitazione e controllo

Un'efficace identificazione dei rischi, che costituisce la base per la limitazione e il controllo dei rischi operativi, considera fattori sia interni[11] che esterni[12]. Comprende almeno le valutazioni del rischio e dei controlli e i risultati della revisione. 128*

A seconda delle attività commerciali specifiche all'istituto e in funzione di tipologia, entità, complessità e tenore del rischio, deve essere esaminata la presa in considerazione di ulteriori strumenti e metodi e all'occorrenza questi ultimi devono essere applicati: 129*

a. rilevamento e analisi di dati di perdita interni;
b. rilevamento e analisi di eventi esterni che sono correlati a rischi operativi;
c. analisi delle interdipendenze tra rischi, processi e controlli;
d. indicatori di rischio e *performance* per il controllo dei rischi operativi e indicatori di efficacia del sistema interno di controllo;
e. analisi di scenario;
f. stima del potenziale di perdita;
g. analisi comparative[13].

La limitazione e il controllo avvengono mediante gli strumenti, le strutture, gli approcci ecc. definiti dalle unità organizzative previste a tale scopo nella strategia quadro per la gestione del rischio a livello di istituto in conformità alla Circolare FINMA 17/1. 130*

d) Principio 3: rendicontazione interna ed esterna

Abrogato 131*

La rendicontazione interna in materia di rischi operativi deve comprendere dati concernenti la finanza, l'esercizio e la *compliance*, ma anche le principali informazioni esterne su eventi e circostanze con rilevanza per i rischi. La rendicontazione sui rischi operativi deve comprendere almeno i seguenti punti e presentare le possibili ripercussioni sull'istituto e il capitale proprio richiesto per i rischi operativi: 132

a. considerevoli violazioni nei confronti della propensione al rischio dell'istituto definita in relazione ai rischi inerenti e residui e superamento delle limitazioni del rischio definite a tal proposito; 132.1*

b. dettagli su fondamentali eventi interni legati ai rischi operativi e/o alle perdite; 132.2*

[11] Per esempio struttura dell'impresa, tipologia delle attività, qualifiche dei collaboratori, cambiamenti sul piano organizzativo e fluttuazione del personale di una banca.
[12] Per esempio cambiamenti a livello dell'ulteriore contesto e del settore come pure progressi tecnologici.
[13] Mediante un'analisi comparativa vengono confrontati i risultati dei diversi strumenti di valutazione per ottenere un quadro maggiormente completo dei rischi operativi della banca.

c. informazioni relative agli eventi esterni che potrebbero essere rilevanti per l'istituto e potenziali rischi, nonché possibili ripercussioni sull'istituto. 132.3*

Un istituto deve disporre di una politica di dichiarazione formale approvata dall'alta direzione, da cui si evince in che modo la banca dichiara i propri rischi operativi e quali processi di controllo devono essere applicati in materia di dichiarazione. 133*

Le informazioni che gli istituti devono dichiarare all'esterno devono consentire ai gruppi di interlocutori di formarsi un'opinione sull'approccio relativo alla gestione dei rischi operativi. Fra questi rientra la strategia di gestione dei rischi operativi. Ciò deve consentire ai gruppi di interlocutori di valutare l'efficacia dell'identificazione, della limitazione e della sorveglianza dei rischi operativi. 134*

e) Principio 4: infrastruttura tecnologica[14]

La direzione generale deve documentare in modo adeguato la gestione dei rischi legati all'infrastruttura informatica in linea con la strategia informatica e la propensione al rischio definita, come pure tenendo conto degli aspetti rilevanti per il rispettivo istituto in conformità agli standard internazionali riconosciuti. 135*

La direzione generale assicura che nella gestione dei rischi legati all'infrastruttura informatica viene tenuto conto almeno dei seguenti aspetti: 135.1*

a. una panoramica attuale delle principali componenti dell'infrastruttura di rete e un inventario di tutte le applicazioni critiche e dell'infrastruttura informatica correlata nonché interfacce con terzi; 135.2*

b. una chiara definizione di ruoli, mansioni e responsabilità per quanto concerne le applicazioni critiche e l'infrastruttura informatica correlata, nonché dati e processi critici e/o sensibili; 135.3*

c. un processo sistematico per quanto riguarda l'identificazione e la valutazione dei rischi informatici nel quadro della dovuta diligenza (due diligence), in particolare nel caso di acquisizioni o di dislocazioni in ambito informatico, come pure nella sorveglianza degli accordi di prestazioni di servizio; 135.4*

d. misure volte a rafforzare la consapevolezza dei collaboratori per quanto concerne la loro responsabilità nel ridurre i rischi informatici nonché il rispetto e il rafforzamento della sicurezza informatica. 135.5*

La direzione generale deve inoltre documentare in modo adeguato la gestione dei rischi cibernetici[15]. La gestione deve coprire almeno i seguenti aspetti e garantire un'effettiva applicazione mediante adeguati processi come pure una chiara definizione di compiti, ruoli e responsabilità: 135.6*

a. identificazione dell'esposizione dell'istituto a potenziali minacce da parte di attacchi 135.7*

[14] Per infrastruttura tecnologica s'intende la struttura (elettronica) fisica e logica dei sistemi informatici e di comunicazione, le singole componenti di hardware e software, i dati e l'ambiente operativo.
[15] Rischi operativi relativi a possibili perdite provocate da attacchi cibernetici.

cibernetici[16], in particolare per quanto riguarda dati e sistemi informatici critici e/o sensibili;

b. tutela dei processi operativi e dell'infrastruttura tecnologica da attacchi cibernetici, in particolare per quanto concerne confidenzialità, integrità e disponibilità dei dati e dei sistemi informatici critici e/o sensibili; 135.8*

c. tempestivo riconoscimento e rilevamento degli attacchi cibernetici sulla base di un processo di sorveglianza sistematica dell'infrastruttura tecnologica; 135.9*

d. reazione agli attacchi cibernetici mediante misure tempestive e mirate, come pure nel caso di attacchi cibernetici importanti, che potrebbero minacciare la prosecuzione della normale attività, in linea con il piano di continuità aziendale (Business Continuity Management, BCM); 135.10*

e. garanzia di un tempestivo ripristino, mediante adeguate misure, della normale attività in seguito ad attacchi cibernetici. 135.11*

Allo scopo di proteggere dati critici e/o sensibili come pure i sistemi informatici da attacchi cibernetici, la direzione generale fa condurre regolarmente analisi della vulnerabilità[17] e *penetration test*[18], che devono essere svolti da personale qualificato dotato di appropriate risorse. 135.12*

f) Principio 5: continuità in caso di interruzione dell'attività

La direzione generale deve disporre di piani di prosecuzione delle attività dell'istituto che garantiscano la continuità delle attività e la delimitazione dei danni in caso di interruzione grave dell'attività.[19] 136*

g) Principio 6: mantenimento di servizi essenziali in caso di liquidazione e di risanamento di banche di rilevanza sistemica

Nel quadro della loro pianificazione d'emergenza, le banche di rilevanza sistemica adottano le misure necessarie volte al mantenimento, senza interruzioni, delle funzioni di rilevanza sistemica (art. 9 cpv. 2 lett. d LBCR in combinato disposto con l'art. 60 segg. OBCR). Le banche identificano i servizi necessari per la prosecuzione delle funzioni di rilevanza sistemica in caso di liquidazione, risanamento o ristrutturazione («prestazioni di servizio cruciali») e adottano le misure necessarie per il loro mantenimento. Al riguardo esse tengono conto delle disposizioni emanate dagli organismi di standardizzazione internazionali in materia. 136.1*

[16] Si tratta di attacchi provenienti da Internet e reti affini che vanno a colpire l'integrità, la disponibilità e la confidenzialità dell'infrastruttura tecnologica, in particolare per quanto riguarda i dati e i sistemi informatici critici e/o sensibili.

[17] Analisi volta a identificare attuali carenze nel software e lacune a livello della sicurezza nell'infrastruttura tecnologica in relazione ad attacchi cibernetici.

[18] Analisi mirata e sfruttamento delle carenze nel software e delle lacune a livello della sicurezza nell'infrastruttura tecnologica, al fine di accedere in maniera abusiva a quest'ultima.

[19] Cfr. le cifre delle raccomandazioni dell'ASB in materia di *Business Continuity Management* (BCM) riconosciute come standard minimo.

h) Principio 7: rischi derivanti da prestazioni di servizio transfrontaliere

Se gli istituti o le relative società del gruppo erogano prestazioni di servizio transfrontaliere o distribuiscono prodotti finanziari, occorre rilevare, limitare e sorveglianza in maniera adeguata i rischi che risultano dall'applicazione della giurisdizione estera (diritto fiscale, penale, in materia di riciclaggio di denaro, ecc.). In particolare, la FINMA, in qualità di autorità di vigilanza, si attende che le banche rispettino il diritto in materia di vigilanza estero. 136.2*

Gli istituti sottopongono i propri servizi finanziari transfrontalieri e la distribuzione transfrontaliera a un'analisi approfondita concernente le condizioni normative quadro da adempiere e i rischi connessi. Sulla base di questa analisi, gli istituti adottano le necessarie misure strategiche e organizzative volte a eliminare e a minimizzare i rischi e le adeguano costantemente alle modificate condizioni. In particolare dispongono del *know-how* necessario specifico al relativo paese, definiscono modelli di prestazioni di servizio *ad hoc* per i paesi in cui queste ultime vengono erogate, istruiscono il proprio personale e, mediante corrispondenti misure organizzative, istruzioni, modelli di remunerazione e sanzioni, garantiscono il rispetto delle direttive. 136.3*

Occorre considerare anche i rischi causati da gestori patrimoniali esterni, da intermediari e da altri prestatori di servizi. Di conseguenza occorre procedere con la massima cura alla scelta e all'istruzione di tali partner. 136.4*

In questo principio rientrano anche i casi in cui una filiale, una succursale o un'entità analoga di un istituto finanziario svizzero con sede all'estero eroga ai clienti servizi transfrontalieri. 136.5*

C. Esigenze qualitative specifiche per il rischio

Il pilotaggio e il controllo dei rischi operativi specifici di considerevole portata deve avvenire in maniera più completa e intensiva rispetto a quanto prescritto dalle esigenze qualitative di base. A tale scopo, la direzione generale deve definire e applicare misure complementari e specifiche al rischio o rafforzare le misure esistenti. 137*

Se la FINMA lo ritiene necessario, per temi specifici può definire ulteriori concretizzazioni in materia di gestione dei rischi operativi. Ciò avviene in maniera ponderata e in applicazione del principio di proporzionalità. Ulteriori esigenze qualitative suddivise per tema sono pubblicate nell'allegato alla presente circolare. 138*

V. Audit e valutazione da parte delle società di audit

Le società di audit verificano il rispetto della presente circolare sulla base della Circ. FINMA 13/3 «Attività di audit» e riportano il risultato dei loro atti di verifica nel rapporto di audit. 139*

Allegato 1

Classificazione degli ambiti di attività conformemente all'art. 93 cpv. 2 OFoP

I. Panoramica

1° livello	2° livello	Attività
Finanziamento / Consulenza d' imprese	Finanziamento / Consulenza d'imprese	Fusioni e acquisizioni, operazioni di emissione e di collocamento, privatizzazioni, cartolarizzazioni, *research*, crediti (enti pubblici, *high yield*), partecipazioni, prestiti consorziali, ingressi in borsa (*initial public offering*), collocamenti privati nel mercato secondario
	Enti pubblici	
	Finanziamenti commerciali	
	Servizi di consulenza	
Negoziazione	Negoziazione per conto di clienti	Obbligazioni, azioni, operazioni su divise, operazioni su materie prime, crediti, prodotti derivati, *funding*, Negoziazione per conto della banca, prestito di titoli e operazioni pronti contro termine (*repo*), *brokerage* (per investitori non *retail*), *prime brokerage*
	Market making	
	Negoziazione per conto della banca	
	Tesoreria	
Attività bancaria al dettaglio per i privati	*Retail banking*	Gestione e operazioni di credito, prestazioni di servizi, operazioni fiduciarie e gestione patrimoniale
	Private banking	Gestione e operazioni di credito, prestazioni di servizi, operazioni fiduciarie, gestione patrimonialee altri servizi di *private banking*
	Servizi di carte	Carte per aziende e privati
Attività bancaria al dettaglio per le ditte	Attività bancaria al dettaglio per le ditte	Finanziamento di progetti, finanziamento di immobili, finanziamento delle esportazioni, finanziamento commerciale, *factoring*, *leasing*, concessione di crediti, garanzie e fideiussioni, operazioni su cambiali
Traffico dei pagamenti / Regolamento dei titoli [20]	Clienti esterni	Traffico dei pagamenti, *clearing* e regolamento titoli per conto di terzi
Attività di deposito e depositi fiduciari	Custodia	Custodia a titolo fiduciario, operazioni di deposito, custodia di titoli, prestito di titoli per clienti; servizi analoghi per aziende
	Operazioni fiduciarie	Funzioni di emittente e agente pagatore
	Fondazioni	
Gestione patrimoniale istituzionale	Gestione patrimoniale libera	Gestione in *pool*, segmentata, relativa alla clientela *retail*, istituzionale, chiusa, aperta, *private equity*
	Gestione patrimoniale vincolata	Gestione in *pool*, segmentata, relativa alla clientela *retail*, individuale, chiusa, aperta
Attività di commissione su titoli	Esecuzione di ordini su titoli	Esecuzione, compresi tutti i servizi collegati

[20] Le perdite subite nel traffico dei pagamenti / regolamento dei titoli concernenti le operazioni proprie di un istituto devono essere imputate alle perdite del rispettivo ambito di attività.

Allegato 1

finma

Classificazione degli ambiti di attività conformemente all'art. 93 cpv. 2 OFoP

II. Principi di assegnazione

1.	Tutte le attività di una banca devono essere interamente assegnate a uno degli otto ambiti di attività (primo livello nella tabella 2), senza sovrapposizioni.	2
2.	Anche le attività a carattere ausiliario che non hanno un rapporto diretto con il *core business* di una banca devono essere attribuite a un ambito di attività. Se il supporto fornito riguarda un solo ambito di attività, si effettuerà l'assegnazione a quest'ultimo. Se invece l'attività a carattere ausiliario viene prestata in diversi ambiti, l'attribuzione sarà effettuata sulla base di criteri oggettivi.	3
3.	Se un'attività non può essere classificata in uno specifico ambito sulla base di criteri oggettivi, deve essere attribuita all'ambito che presenta il fattore β più alto tra quelli che entrano in linea di conto. Ciò vale anche per le attività a carattere ausiliario.	4
4.	Le banche possono applicare metodi interni di computazione per l'assegnazione del loro indicatore di ricavo GI. In ogni caso, tuttavia, la somma degli indicatori di ricavo degli otto ambiti di attività deve corrispondere all'indicatore di ricavo valido per l'intera banca, come viene utilizzato nell'approccio dell'indicatore di base.	5
5.	La classificazione delle attività nei singoli ambiti per il calcolo delle esigenze di fondi propri per i rischi operativi deve essere, in generale, compatibile con i criteri utilizzati per la delimitazione dei rischi di credito e di mercato. Eventuali deroghe a questo principio devono essere chiaramente motivate e documentate.	6
6.	L'insieme dei processi di classificazione deve essere documentato in modo trasparente. In particolare, le definizioni scritte degli ambiti di attività devono essere sufficientemente chiare e dettagliate per consentirne la comprensione anche ai non addetti ai lavori. Le eventuali eccezioni ai principi di classificazione devono essere anch'esse chiaramente motivate e documentate.	7
7.	La banca deve disporre di procedure che le consentano di classificare nuove attività o nuovi prodotti.	8
8.	La direzione generale è responsabile dei criteri di classificazione. Questi sono soggetti all'approvazione dell'organo preposto all'alta direzione, alla vigilanza e al controllo della banca.	9*
9.	Le procedure di classificazione devono essere periodicamente verificate da parte della società di audit.	10

Allegato 2

Panoramica della categorizzazione dei tipi di eventi

Categoria di evento di perdita (livello 1)	Definizione	Sottocategorie (livello 2)	Esempi di attività (livello 3)
Frode interna	Perdite dovute ad atti compiuti con intenzioni fraudolente, appropriazione indebita di beni, aggiramento di leggi, prescrizioni o disposizioni interne (con implicazione di almeno una parte interna all'azienda)	Attività non autorizzata	Transazioni non notificate (intenzionalmente) Transazioni non autorizzate (con danno finanziario) False registrazioni di posizioni (intenzionalmente)
		Furto e frode	Frode, frode creditizia, depositi senza valore Furto, estorsione, appropriazione indebita, rapina Appropriazione indebita di valori patrimoniali Distruzione dolosa di valori patrimoniali Falsificazioni Falsificazione di assegni Contrabbando Accesso non autorizzato a conti di terzi Reati fiscali Corruzione *Insider trading* (non per conto del datore di lavoro)
Frode esterna	Perdite dovute ad atti compiuti con intenzioni fraudolente, appropriazione indebita di beni, aggiramento di leggi o prescrizioni (senza	Furto e frode	Furto, rapina Falsificazioni Falsificazione di assegni

Allegato 2

Panoramica della categorizzazione dei tipi di eventi

Categoria di evento di perdita (livello 1)	Definizione	Sottocategorie (livello 2)	Esempi di attività (livello 3)
	implicazione di una parte interna all'azienda)	Sicurezza informatica	Danni provocati da *hacker* Accesso non autorizzato a informazioni (con danno finanziario)
Posto di lavoro	Perdite derivanti da violazioni di disposizioni legali relative al lavoro o di prescrizioni o convenzioni relative alla sicurezza o alla salute, ivi compreso l'insieme dei pagamenti collegati a tali violazioni	Collaboratori	Pagamenti compensatori e di indennizzo, perdite relative a scioperi, ecc.
		Sicurezza sul posto di lavoro	Responsabilità civile generale Violazione di disposizioni relative alla sicurezza e alla salute del personale Indennizzi o risarcimenti a collaboratori
		Discriminazione	Risarcimenti da corrispondere a titolo di azioni per discriminazione

Allegato 2

Panoramica della categorizzazione dei tipi di eventi

Categoria di evento di perdita (livello 1)	Definizione	Sottocategorie (livello 2)	Esempi di attività (livello 3)
Clienti, prodotti e pratiche commerciali	Perdite derivanti dal mancato adempimento, non intenzionale né dovuto a negligenza, di obblighi verso clienti e perdite derivanti dal tipo o dalla struttura di determinati prodotti	Adeguatezza, pubblicazione di informazioni e obblighi fiduciari	Violazione di obblighi fiduciari, trasgressione di direttive Problemi relativi all'adeguatezza e alla pubblicazione di informazioni (regole *know-your-customer*, ecc.) Violazione di obblighi di informazione nei confronti dei clienti Violazione del segreto bancario o di disposizioni relative alla protezione dei dati Pratiche di vendita aggressive Creazione indebita di pagamenti di commissioni e di provvigioni di mediazione Abuso di informazioni confidenziali Responsabilità del creditore

Allegato 2

Panoramica della categorizzazione dei tipi di eventi

Categoria di evento di perdita (livello 1)	Definizione	Sottocategorie (livello 2)	Esempi di attività (livello 3)
		Pratiche commerciali o di mercato illecite	Violazione delle disposizioni antitrust Pratiche di mercato illecite Manipolazione del mercato *Insider trading* (per conto del datore di lavoro) Esercizio di attività senza la relativa autorizzazione Riciclaggio di denaro
		Problemi con prodotti	Problemi causati dai prodotti (mancanza di autorizzazione, ecc.) Errori di modelli
		Selezione dei clienti, assegnazione di operazioni ed esposizione creditizia	Procedure di analisi della clientela non compatibili con le direttive interne Superamento di limiti
		Attività di consulenza	Contenziosi sorti in merito ai risultati relativi all'attività di consulenza
Danni materiali	Perdite derivanti da danni a beni patrimoniali fisici a causa di catastrofi naturali o altri eventi	Catastrofi e altri eventi	Catastrofi naturali Terrorismo Vandalismo
Interruzioni dell'attività e anomalie dei sistemi	Perdite derivanti da interruzioni dell'attività o problemi con sistemi tecnici	Sistemi tecnici	Hardware Software Telecomunicazioni Blackout, ecc.

Allegato 2

Panoramica della categorizzazione dei tipi di eventi

Categoria di evento di perdita (livello 1)	Definizione	Sottocategorie (livello 2)	Esempi di attività (livello 3)
Esecuzione, fornitura e gestione dei processi	Perdite derivanti da errori nell'esecuzione di attività o nella gestione dei processi; perdite derivanti da relazioni con partner commerciali, fornitori, ecc.	Registrazione, esecuzione e assistenza in materia di transazioni	Errori di comunicazione Errori nella registrazione o nella manutenzione dei dati Inosservanza dei termini Mancato adempimento di un compito Errori nell'applicazione di modelli o sistemi Errori contabili o attribuzione all'unità sbagliata Fornitura errata o non avvenuta Gestione errata degli strumenti di copertura Errori nella gestione dei dati di riferimento Errori in altre mansioni
		Sorveglianza e notifiche	Mancato adempimento degli obblighi di notifica Rapporti inadeguati destinati a esterni (con conseguenti perdite)
		Accettazione della clientela e relativa documentazione	Mancato rispetto delle relative prescrizioni interne ed esterne

Allegato 2

Panoramica della categorizzazione dei tipi di eventi

Categoria di evento di perdita (livello 1)	Definizione	Sottocategorie (livello 2)	Esempi di attività (livello 3)
		Tenuta dei conti per i clienti	Concessione di un accesso al conto non legittimato Gestione non corretta del conto (con conseguenti perdite) Perdita o danneggiamento di valori patrimoniali dei clienti dovuti a negligenza
		Partner commerciali	Prestazione errata di partner commerciali (non clienti) Controversie varie con partner commerciali (non clienti)
		Fornitori e offerenti	*Outsourcing* Controversie con fornitori e offerenti

Allegato 3*

Trattamento dei dati elettronici dei clienti

Nel presente allegato sono elencati i principi e le relative precisazioni concernenti un'adeguata gestione dei rischi in relazione alla confidenzialità dei dati elettronici delle persone fisiche («clienti privati»[21]) le cui relazioni commerciali sono seguite e gestite in o a partire dalla Svizzera («dati di clienti»). I principi si orientano principalmente al rischio di incidenti in riferimento alla confidenzialità di una grande quantità di dati dei clienti attraverso l'utilizzo di sistemi elettronici. Essi affrontano solo in maniera marginale le considerazioni sulla sicurezza dei dati fisici o le questioni di integrità e disponibilità dei dati. Le disposizioni giuridiche pertinenti trovano il loro fondamento non solo nel diritto in materia di vigilanza[22], ma anche nella legislazione relativa alla protezione dei dati[23] e nel diritto civile. 1*

Le banche di piccole dimensioni[24] sono esonerate dall'adempimento dei seguenti numeri marginali: 2*

- nm. 15–19 e 22 del principio 3;
- tutti i numeri marginali dei principi 4–6;
- nm. 41 del principio 7.

Per quanto concerne l'applicazione dei requisiti di cui all'allegato 3, gli istituti secondo gli artt. 47*a*–47*e* OFoP come pure gli istituti secondo l'art.1*b* LBCR possono limitarsi al nm. 3. L'applicazione del requisito di cui al nm. 3 dipende dalle dimensioni, dalla complessità, dalla struttura e dal profilo di rischio dell'istituto. 2.1*

I. Principi per un'adeguata gestione dei rischi in relazione alla confidenzialità dei dati dei clienti

A. Principio 1: *governance*

I rischi legati alla confidenzialità dei dati dei clienti vengono sistematicamente identificati, limitati e sorvegliati. A tale scopo, l'alta direzione sorveglia la direzione generale per assicurare un'implementazione efficace delle misure volte a garantire la confidenzialità dei dati dei clienti. La direzione generale incarica un'unità indipendente, che svolge la funzione di controllo, di realizzare e mantenere le condizioni quadro che garantiscono la confidenzialità dei dati dei clienti. 3*

a) Indipendenza e responsabilità

L'unità competente della realizzazione e del mantenimento delle condizioni quadro tese a garantire la confidenzialità dei dati dei clienti deve essere indipendente dalle unità responsabili dell'elaborazione dei dati. 4*

[21] Per «clienti privati» si intendono anche le relazioni commerciali in cui la persona fisica instaura una relazione commerciale con la banca mediante una persona giuridica (p. es. in qualità di avente diritto economico di società di sede, società di domicilio, fondazione) o mediante un *trust*.
[22] In particolare art. 3 e 47 LBCR e art. 12 OBCR; art. 10 e 43 LBVM e art. 19 seg. OBVM.
[23] In particolare art. 7 LPD e art. 8 segg. OLPD (cfr. anche le guide dell'IFPDT).
[24] Cfr. nm. 118

Devono essere definite le responsabilità per tutte le funzioni e i siti interessati e realizzate chiare strutture di *escalation* delle informazioni. In particolare, la determinazione delle responsabilità e la loro ripartizione tra funzioni di *front-office*, tecnologia informatica e di controllo devono essere definite dalla direzione generale e approvate dall'alta direzione. La direzione generale informa regolarmente l'alta direzione in merito all'efficacia dei controlli effettuati. 5*

b) Direttive, processi e sistemi

Si presuppone che sussista una strategia quadro formale e completa concernente le attività, i processi e i sistemi che garantiscono la confidenzialità dei dati, la cui struttura tenga conto delle dimensioni e della complessità della banca. La strategia deve essere applicata in maniera coerente in tutti gli ambiti funzionali e in tutte le unità che hanno accesso o trattano dati dei clienti. 6*

Devono essere stabilite per iscritto in maniera comprensibile e vincolante le misure che tengono conto della tolleranza al rischio definite dalla banca e la periodicità della relativa attuazione. 7*

L'implementazione e il rispetto della strategia quadro concernente la confidenzialità dei dati dei clienti sono sottoposti alla sorveglianza dell'alta direzione e devono essere garantiti mediante controlli regolari della confidenzialità e della sicurezza dei dati da parte dell'unità competente. 8*

B. Principio 2: dati di identificazione del cliente (*Client Identifying Data*, CID)

Il requisito fondamentale alla base di un'adeguata strategia quadro tesa a garantire la confidenzialità dei dati dei clienti consiste nella categorizzazione dei dati dei clienti che una banca tratta. Ciò richiede la definizione specifica a livello di impresa dei dati di identificazione dei clienti (CID) e la loro classificazione in base al livello di confidenzialità e protezione. Inoltre, occorre disciplinare l'attribuzione della responsabilità dei dati (*Data Owners*). 9*

a) Categorie di dati di clienti e definizione dei CID

In seno alla banca deve essere disponibile e documentato a livello formale un elenco chiaro e trasparente delle categorie di dati dei clienti, che includa la definizione dei CID specifica all'impresa. La categorizzazione e la definizione dei dati dei clienti deve comprendere tutti i dati suscettibili di diretta identificazione del cliente (p. es. nome, secondo nome, cognome), i dati suscettibili di indiretta identificazione del cliente (p. es. numero di passaporto) e i dati potenzialmente suscettibili di indiretta identificazione del cliente (p. es. combinazioni di data di nascita, professione, nazionalità, ecc.). 10*

Ogni banca deve disporre di una categorizzazione e di una propria definizione dei CID che risulti adeguata alla sua clientela specifica. 11*

b) Classificazione dei CID e livelli di confidenzialità

I CID devono essere suddivisi in livelli di confidenzialità in base a criteri formali di classificazione. Ai fini della protezione dei dati, la classificazione dei dati dei clienti deve 12*

contenere chiari requisiti concernenti l'accesso e le corrispondenti misure tecniche (p. es. anonimizzazione, cifratura e pseudonimizzazione) e distinguere in linea di massima diversi livelli di confidenzialità e protezione.

c) Responsabilità dei CID

Devono essere definiti criteri per l'attribuzione della responsabilità dei dati applicabili in egual misura a tutte le unità che hanno accesso o elaborano CID. Le unità responsabili dei CID (*Data Owners)* devono assumere la sorveglianza dell'intero ciclo di vita dei dati dei clienti, compresa l'approvazione dei diritti di accesso come pure la soppressione e lo smaltimento di tutti i sistemi operativi e di backup. 13*

Le unità responsabili dei CID (*Data Owners)* sono competenti dell'implementazione delle direttive di classificazione dei dati come pure della giustificazione e della documentazione delle eccezioni. 14*

C. Principio 3: luogo di stoccaggio e accesso ai dati

La banca deve essere a conoscenza del luogo in cui sono stoccati i CID, le applicazioni e i sistemi informatici con i quali questi ultimi vengono trattati e dove è possibile accedervi in via elettronica. Occorre garantire mediante adeguati controlli il trattamento dei dati in conformità all'art. 8 segg. dell'Ordinanza relativa alla legge federale sulla protezione dei dati. Sono necessari controlli speciali per i settori fisici (p. es. *server room*) o le zone di rete in cui è stoccata o resa accessibile una grande quantità di dati di CID. L'accesso ai dati deve essere chiaramente regolamentato e può avvenire solo su una rigida base *need to know*. 15*

a) Luogo di stoccaggio e accesso ai dati in generale

Deve essere disponibile e costantemente aggiornato un inventario delle applicazioni e della relativa infrastruttura che contengono o elaborano CID. L'inventario deve essere immediatamente aggiornato in particolare in caso di modifiche strutturali (p. es. nuovi siti o rinnovamento dell'infrastruttura tecnica). Le modifiche di modesta entità devono essere apportate regolarmente. 16*

Si presuppone che il grado di dettaglio dell'inventario consenta alla banca di determinare: 17*

- dove sono stoccati i CID, mediante quali applicazioni e sistemi informatici sono trattati e il luogo in cui è possibile accedervi in via elettronica (applicazioni degli utenti finali); 18*
- siti e unità giuridiche a livello nazionale e internazionale da cui è possibile accedere ai dati (comprese le prestazioni di servizio esternalizzate e le società esterne). 19*

b) Luogo di stoccaggio e accesso ai dati dall'estero

Se i CID vengono stoccati al di fuori della Svizzera oppure vi si accede dall'estero, i rischi superiori che ne derivano a livello della protezione dei dati dei clienti devono essere 20*

adeguatamente limitati.[25] I CID devono essere protetti in maniera adeguata (p. es. anonimizzati, cifrati o pseudoanonimizzati).

c) Principio need to know

Le persone devono avere accesso unicamente alle informazioni e alle funzionalità necessarie all'esercizio dei loro compiti. 21*

d) Diritti di accesso

La banca deve disporre di un sistema di autorizzazione fondato sulle funzioni e i ruoli che disciplini in maniera univoca i diritti di accesso dei collaboratori e dei terzi al CID. Per garantire l'accesso ai CID solo da parte delle persone che beneficiano di un'autorizzazione valida, devono essere regolarmente confermati i diritti di accesso. 22*

D. Principio 4: standard di sicurezza per l'infrastruttura e la tecnologia

Gli standard di sicurezza per l'infrastruttura e la tecnologia impiegati per la protezione della confidenzialità dei CID devono essere adeguati alla complessità della banca e all'esposizione ai rischi di quest'ultima e garantire la protezione dei CID a livello di terminale (al punto terminale) come pure nella trasmissione e stoccaggio di CID. Poiché le tecnologie dell'informazione sottostanno a rapide modifiche, occorre seguire attentamente l'evoluzione delle soluzioni per la sicurezza dei dati. È necessario valutare regolarmente il divario tra la strategia quadro interna in vigore tesa a garantire la confidenzialità dei dati dei clienti e la prassi di mercato. 23*

a) Standard di sicurezza

Gli standard di sicurezza devono essere adeguati alle dimensioni della banca e al grado di complessità della sua architettura informatica. 24*

b) Standard di sicurezza e prassi di mercato

Gli standard di sicurezza costituiscono una parte integrante fissa della strategia quadro che garantiscono la confidenzialità dei dati dei clienti. Devono essere regolarmente confrontati con la prassi di mercato al fine di individuare possibili lacune a livello di sicurezza. Devono essere presi in considerazione anche gli input esterni sotto forma di verifiche indipendenti e rapporti di audit. 25*

c) Sicurezza nella trasmissione di CID e a livello dei CID registrati sul terminale (punto terminale)

Per garantire la confidenzialità dei CID, la banca deve valutare misure di protezione (p. es. cifratura) e applicarle, dove necessario, ai seguenti livelli: 26*

[25] Occorre inoltre rispettare le pertinenti disposizioni del diritto in materia di protezione dei dati, come l'art. 6 LPD.

a) sicurezza dei CID sul terminale e al punto terminale (p. es. PC, notebook, supporti dati portatili e apparecchi mobili); 27*

b) sicurezza nella trasmissione dei CID (p. es. all'interno di una rete o fra diversi siti); 28*

c) sicurezza dei CID stoccati (p. es. in server, banche dati o sistemi di backup). 29*

E. Principio 5: selezione, sorveglianza e formazione dei collaboratori che hanno accesso ai CID

Collaboratori con una buona formazione e coscienti della propria responsabilità rappresentano un elemento centrale per l'attuazione di misure efficaci a livello di impresa tese a garantire la protezione della confidenzialità dei dati dei clienti. I collaboratori che hanno accesso ai CID devono pertanto essere accuratamente selezionati, formati e sorvegliati. Ciò vale anche per i terzi che possono accedere ai CID su mandato della banca. Occorre applicare requisiti più stringenti in materia di sicurezza per informatici e utenti (altamente) privilegiati (p. es. amministratori di sistema) che nella loro funzione accedono a una grande quantità di CID («collaboratori chiave»), ai quali è necessario prestare particolare attenzione. 30*

a) Accurata selezione dei collaboratori

I collaboratori che possono accedere ai CID devono essere accuratamente selezionati. In particolare, preventivamente all'avvio dell'attività occorre verificare che il potenziale collaboratore adempia i requisiti per un appropriato trattamento dei CID. Inoltre, la banca deve disciplinare in via contrattuale le modalità in base alle quali i collaboratori sono selezionati da terzi o designati da imprese terze che, su mandato della banca, possono accedere ai CID, affinché tutti i collaboratori siano accuratamente selezionati nel quadro di un processo comparabile. 31*

b) Formazioni mirate dei collaboratori

I collaboratori interni ed esterni devono essere sensibilizzati alle questioni relative alla sicurezza dei dati dei clienti nel quadro di formazioni mirate. 32*

c) Requisiti in materia di sicurezza

La banca deve disporre di chiari requisiti in materia di sicurezza per i collaboratori che hanno accesso ai CID e verificare periodicamente se sono sempre adempiuti i requisiti relativi a un trattamento adeguato dei CID. Devono essere applicati requisiti più severi in materia di sicurezza per informatici e utenti (altamente) privilegiati che nella loro funzione accedono in maniera funzionale[26] a una grande quantità di CID («collaboratori chiave»). 33*

[26] Nel caso di diritti di accesso ampliati, p. es. consultazione ed estrazione/migrazione di una grande quantità di CID.

d) Lista di collaboratori chiave

In via integrativa ai requisiti generali relativi ai diritti di accesso per collaboratori e terzi (v. nm. 22), la banca deve tenere e aggiornare continuamente una lista con i nomi di tutti gli informatici e utenti (altamente) privilegiati interni ed esterni («collaboratori chiave») che hanno accesso a una grande quantità di CID[27] e/o ai quali sono state trasferite responsabilità in materia di controllo e sorveglianza della confidenzialità dei dati dei clienti. 34*

Devono essere introdotte misure, come ad esempio la gestione di *log files,* che consentano di identificare gli utenti che accedono a una grande quantità di CID. 35*

F. Principio 6: identificazione e controllo del rischio in riferimento alla confidenzialità dei CID

L'unità competente della confidenzialità e della sicurezza dei dati identifica e valuta i rischi inerenti e i rischi residui concernenti la confidenzialità dei CID mediante un processo strutturato. Tale processo deve comprendere gli scenari di rischio[28] in relazione alla confidenzialità dei CID, pertinenti per la banca, e la definizione dei controlli chiave corrispondenti. Il catalogo dei controlli chiave in relazione alla confidenzialità dei dati, teso a garantire la protezione dei CID, deve essere costantemente verificato dal punto di vista dell'adeguatezza e, all'occorrenza, adeguato. 36*

a) Processo di valutazione del rischio

La valutazione del rischio inerente alla confidenzialità dei CID e del rischio residuo deve avvenire sulla base di un processo strutturato e con il coinvolgimento delle funzioni operative, informatiche e di controllo. 37*

b) Scenari di rischio e controlli chiave[29]

La definizione degli scenari di rischio e dei corrispondenti controlli chiave in relazione alla confidenzialità dei CID devono essere commisurati all'esposizione al rischio e alla complessità della banca e devono essere periodicamente rivisti. 38*

G. Principio 7: diminuzione del rischio in relazione alla confidenzialità dei CID

I rischi identificati devono essere sorvegliati e limitati in maniera appropriata. Ciò vale in particolare per le attività di elaborazione dei dati nel corso delle quali viene modificata o migrata una grande quantità di CID.[30] Nel caso di cambiamenti strutturali (p. es. riorganizzazioni di 39*

[27] Singole consultazioni con diritti di accesso limitati (p. es. operatori di sportello) non rientrano del concetto di accesso a una grande quantità di CID.

[28] Sulla base di un'analisi degli incidenti gravi legati alla sicurezza dei dati che si sono verificati presso la banca o presso un concorrente, o di una descrizione di incidenti gravi puramente ipotetici.

[29] Le pratiche di mercato concernenti gli scenari relativi alla sicurezza e i relativi controlli chiave sono trattati in maniera approfondita dall'Associazione svizzera dei banchieri con il titolo «Data Leakage Protection – Information on Best Practice by the Working Group Information Security of the Swiss Bankers Association» (ottobre 2012).

[30] Tale scenario si configura di norma al momento dell'ulteriore sviluppo, della modifica o della migrazione dei sistemi in ragione di aggiornamenti sul piano tecnologico o di ristrutturazioni a livello organizzativo.

ampio respiro), la banca deve prendere in considerazione tempestivamente e scrupolosamente le misure di sicurezza che garantiscono la confidenzialità dei CID.

a) Contesto di produzione, elaborazione dei dati in relazione a una grande quantità di CID

L'elaborazione dei dati, che nel contesto produttivo concerne una grande quantità di CID non anonimizzati, non criptati e non pseudonomizzati, deve essere sottoposta a consone procedure (p. es. principio del doppio controllo o *log files*), compresa la notifica all'unità competente per la sicurezza e la confidenzialità dei dati. 40*

b) Test per lo sviluppo, le modifiche e la migrazione dei sistemi

Durante lo sviluppo, la modifica e la migrazione dei sistemi, i CID devono essere adeguatamente protetti dall'accesso e l'utilizzo da parte di soggetti non autorizzati. 41*

Se un istituto, durante lo sviluppo, la modifica e la migrazione di sistemi (p. es. nella generazione di dati di test o nello stoccaggio intermedio di dati durante la migrazione di questi ultimi), non ricorre ad alcun metodo per anonimizzare, pseudonimizzare o criptare i dati (lavori «in testo in chiaro»), applica per queste attività le disposizioni di cui al nm. 40. 41.1*

H. Principio 8: incidenti legati alla confidenzialità dei CID, comunicazione interna ed esterna

Ci si attende che le banche introducano processi predefiniti per contrastare rapidamente incidenti legati alla confidenzialità, compresa una chiara strategia di comunicazione degli incidenti gravi. Inoltre, le eccezioni, gli incidenti e i risultati degli audit e dei controlli devono essere sorvegliati, analizzati e notificati in maniera appropriata al management di massimo grado. Tale procedura deve contribuire a migliorare in maniera permanente le misure destinate a garantire la confidenzialità dei CID. 42*

a) Identificazione degli incidenti legati alla confidenzialità e reazione

Occorre formalizzare un processo chiaramente definito per l'identificazione degli incidenti in relazione alla confidenzialità e la conseguente reazione, nonché comunicarlo a tutte le parti interessate in seno all'istituto. 43*

b) Notifica

È necessario che il rischio legato alla violazione della confidenzialità dei CID e le relative notifiche di *compliance* siano presentati in maniera adeguata nei rapporti interni oppure, in alternativa, che il rilevamento sistematico e l'*escalation* agli opportuni organi siano garantiti se il segreto legato a tali eventi lo impone. 44*

c) Miglioramento permanente del quadro che garantisce la confidenzialità dei CID

La strategia quadro tesa a garantire la confidenzialità dei CID (nm. 6, 7 e 8) e gli standard di sicurezza devono essere periodicamente controllati. Gli incidenti, le eccezioni e i risultati dei controlli e degli audit devono contribuire a un miglioramento permanente della strategia quadro. 45*

d) Comunicazione esterna

La banca deve disporre di una chiara strategia di comunicazione nel caso in cui si verifichino incidenti gravi legati alla confidenzialità dei CID. Occorre segnatamente disciplinare la forma e il momento preciso della comunicazione alla FINMA, alle autorità di perseguimento penale, ai clienti interessati e ai mass media. 46*

I. Principio 9: esternalizzazione di attività e prestazioni di servizio su grande scala in relazione ai CID

La confidenzialità dei CID deve costituire un criterio determinante al momento della scelta dei fornitori di prestazioni di servizio esternalizzate che trattano i CID ed essere parte integrante dell'esame della *due diligence* soggiacente. In conformità alla Circ. FINMA 08/7 «Outsourcing – banche», la banca continua ad assumere la responsabilità finale dei CID durante la totalità del ciclo di vita delle prestazioni di servizio esternalizzate. I requisiti seguenti si applicano imperativamente a tutte le tipologie di attività che implicano l'accesso a una grande quantità di CID e comprendono anche le prestazioni di servizio su grande scala (p. es. prestatori terzi di servizi informatici, supporto per l'installazione e manutenzione delle piattaforme informatiche sviluppate all'esterno, *hosting* delle applicazioni) e prestazioni di servizio che esulano dall'ambito informatico (p. es. esternalizzazione di eventi per clienti, ecc.). 47*

a) Obbligo di diligenza in relazione alla confidenzialità dei CID (*due diligence)*

L'obbligo di diligenza in relazione alla confidenzialità dei CID deve essere parte integrante del processo di selezione dei fornitori di servizi esternalizzati e dei fornitori di prestazioni di servizio su grande scala. Occorre definire chiari criteri per la valutazione degli standard di sicurezza e di confidenzialità di tali terzi. L'esame concernente gli standard di sicurezza e di confidenzialità dei CID deve essere realizzato preventivamente all'accordo contrattuale e periodicamente reiterato. 48*

b) Obbligo di diligenza in relazione alla confidenzialità dei CID (*due diligence)* e accordi di prestazioni di servizio

I terzi devono essere informati sugli standard di sicurezza e di confidenzialità interni alla banca e su una loro eventuale estensione e osservarli come requisito minimo. 49*

c) Responsabilità generale

Per ognuna delle attività esternalizzate che prevedono l'accesso ai CID, la banca deve designare almeno un collaboratore interno responsabile del rispetto degli standard di sicurezza e confidenzialità in relazione alla confidenzialità dei CID. 50*

d) Organizzazione dei controlli e dei test di efficacia

La banca deve sapere e comprendere quali controlli chiave deve effettuare il fornitore di servizi esternalizzati in relazione alla confidenzialità dei CID. Il rispetto dei requisiti interni e l'efficacia dei controlli devono essere controllati e valutati. 51*

II. Glossario

Dati di identificazione del cliente (*Client Identifying Data*, CID): dati di clienti che costituiscono dati personali ai sensi dell'art. 3 lett. a LPD e consentono di identificare i clienti interessati. 52*

Grande quantità di CID: quantità di CID significativa rispetto al numero totale dei conti / alla dimensione totale del portafoglio di clienti privati. 53*

Prestazioni di servizio su grande scala: tutte le prestazioni di servizio fornite da terzi che richiedono o potenzialmente consentono l'accesso a una grande quantità di CID (p. es. nell'implementazione dei profili di diritti di accesso effettuata da collaboratori appartenenti a terzi). Un rischio legato ai CID può per esempio verificarsi al momento dell'installazione di applicazioni o dell'implementazione di parametri locali (p. es. diritti di accesso), nello stoccaggio dei dati o durante la manutenzione corrente del sistema (p. es. prestatari terzi di servizi informatici, piattaforme informatiche sviluppate all'esterno). Ciò comprende anche le attività interne di audit e gli audit esterni. In genere, le prestazioni di servizio su grande scala sono orientate al lungo termine. 54*

Collaboratori per conto di terzi: tutti i collaboratori che lavorano per conto di incaricati della banca (p. es. mandatari, consulenti, auditor esterni, supporto esterno, ecc.) che hanno accesso ai CID e non sono collaboratori interni. 55*

Collaboratori chiave: tutti i collaboratori interni ed esterni che operano nel settore informatico e in altri settori dell'impresa e che, in ragione del loro profilo di attività e dei loro compiti, dispongono di un accesso (altamente) privilegiato a grandi quantità di CID (p. es. amministratori di banche dati, membri del management di massimo grado). 56*

Incidente grave relativo alla confidenzialità dei dati dei clienti / perdita di una grande quantità di dati dei clienti: un incidente relativo alla confidenzialità dei dati di clienti che comporta una perdita significativa di CID (rispetto al numero totale dei conti / alle dimensioni complessive del portafoglio di clienti). 57*

Controllo chiave: controllo che, se definito, implementato ed eseguito a regola d'arte, consente di ridurre notevolmente il rischio di violazione della confidenzialità dei CID. 58*

Rischio inerente: rischio valutato prima dell'attuazione delle misure di attenuazione o di controllo. 59*

Rischio residuo: rischio valutato dopo l'attuazione delle misure di attenuazione o di controllo. 60*

Allegato 3*

Trattamento dei dati elettronici dei clienti

Tecniche reversibili di trattamento dei dati: 61*

- Dati pseudonimizzati (pseudonimizzazione): per pseudonimizzazione si intende il processo di separazione dei dati identificativi (p. es. nome, foto, indirizzo e-mail, numero di telefono) dagli altri dati (p. es. situazione del conto, solvibilità). L'anello di congiunzione tra le due sfere di dati costituiscono i cosiddetti pseudonimi e una regola di attribuzione (tabella di concordanza). Per esempio, gli pseudonimi possono essere creati mediante un generatore di cifre aleatorie e, all'occorrenza, attribuiti a dati personali che consentono l'identificazione mediante una tabella di concordanza. 62*

- Dati cifrati: nella pratica, la pseudonimizzazione può essere realizzata anche mediante un processo di cifratura. In questo caso, lo pseudonimo viene generato mediante la cifratura di dati personali che consentono l'identificazione tramite una chiave crittografica. La reidentificazione avviene, in ragione della cifratura, mediante la chiave segreta. 63*

Tecniche irreversibili di elaborazione dei dati: 64*

Dati anonimizzati: al momento dell'anonimizzazione dei dati personali, tutti gli elementi che consentono l'identificazione di una persona sono eliminati o modificati in maniera irreversibile (p. es. tramite cancellazione o aggregazione), in modo che i dati non possano più essere correlati a una persona identificata o identificabile. In conformità alla definizione, questi dati non sono / non contengono più CID e non rientrano più nella LPD[31]. 65*

[31] Cfr. IFPDT, allegato alle direttive sui requisiti minimi del sistema di protezione dei dati, 5.

Elenco delle modifiche

Questa circolare è modificata come segue:

Modifiche del 1° giugno 2012 entrate in vigore il 1° gennaio 2013.

nm. modificato	84

Sono stati modificati i rimandi all'Ordinanza sui fondi propri (OFoP; RS 952.03) nella versione che entrerà in vigore il 1.1.2013.

Modifica del 29 agosto 2013 entrata in vigore il 1° gennaio 2014.

nm. modificato	116

Modifiche del 29 agosto 2013 entrate in vigore il 1° gennaio 2015.

nuovi nm.	2.1, 117–139
nm. modificati	1, 29, 50, 53, 71, 79
nm. abrogati	20–22, 28, 30–44, 64
altre modifiche	Nuovo titolo principale precedente al nm. 3 e nuova strutturazione dei titoli Modifica del titolo precedente al nm. 50

Modifiche del 27 marzo 2014 entrate in vigore il 1° gennaio 2015.

nm. modificati	1, 9, 10, 11, 12, 13, 14

Modifiche del 22 settembre 2016 che entrano in vigore il 1° luglio 2017.

nuovi nm.	132.1–132.3, 135.1–135.12, 136.1–136.5
nm. modificati	2, 53, 117–119, 121–122, 128–130, 132–137
nm. abrogati	2.1, 123–127, 131
altre modifiche	Ristrutturazione dei principi

Modifiche del 31 ottobre 2019 in vigore dal 1° gennaio 2020.

nm. modificati	122, 135, 135.1, 135.6

Gli allegati alla circolare sono modificati come segue:

Modifiche del 29 agosto 2013 che entrno in vigore il 1° gennaio 2015.

La numerazione degli allegati viene adeguata: l'allegato 2 «Classificazione degli ambiti di attività conformemente all'art. 93 cpv. 2 OFoP» diventa ora l'allegato 1 e l'allegato 3 «Panoramica della catalogazione dei tipi di eventi» diventa ora l'allegato 2.

Elenco delle modifiche

nuovo	Allegato 3
abrogati	Allegati 1 e 4

Modifiche del 22 settembre 2016 che entrano in vigore il 1° luglio 2017.

nuovi nm.	Allegato 3: 41.1
nm. modificati	Allegato 3: 2, 3, 5–7, 8, 16, 17, 30, 33, 34, 56

Modifica del 31 ottobre 2019 in vigore dal 1° gennaio 2020.

nuovo nm.	Allegato 3: 2.1