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 2023/1
Rischi operativi e resilienza – banche

Gestione dei rischi operativi e garanzia della resilienza operativa

Riferimento:	Circ. FINMA 23/1 «Rischi operativi e resilienza – banche»
Data:	7 dicembre 2022
Entrata in vigore:	1° gennaio 2024
Concordanza:	sostituisce la Circ. FINMA 08/21 «Rischi operativi – banche» del 20 novembre 2008
Basi legali:	LFINMA art. 7 cpv. 1 lett. b e art. 29 cpv. 1 LBCR art. 1*b* cpv. 3 lett. b, art. 3 cpv. 2 lett. a e art. 3*f* OBCR artt. 12 e 14*e* LIsFi artt. 9 e 49 OIsFi artt. 12 e 68
Allegato 1:	Grafico esplicativo sulla resilienza operativa

Destinatari																																			
LBCR			**LSA**			**LIsFi**							**LInFi**						**LICol**							**LRD**		**Altro**								
Banche	Gruppi e congl. finanziari	Altri intermediari	Assicuratori	Gruppi e congl. assicurativi	Intermediari assicurativi	Gestori patrimoniali	Trustee	Gestori di patrimoni collettivi	Direzioni dei fondi	Società di intermed. mobiliare che tengono conti	Società di intermed. mobiliare che non tengono conti		Sedi di negoziazione	Controparti centrali	Depositari centrali	Repertori di dati sulle negoziazioni	Sistemi di pagamento	Partecipanti	SICAV	Società in accomandita per ICC	SICAF	Banche depositarie	Rappresentanti di ICC esteri	Altri intermediari		OAD	Assoggettati affiliati a un OAD	Società di audit	Agenzie di rating						
X	X									X	X																								

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

Indice

I. Oggetto e campo di applicazione

La presente circolare si riferisce alle prescrizioni dell'Ordinanza sulle banche (artt. 12 e 14*e* OBCR; RS 952.02) e dell'Ordinanza sugli istituti finanziari (artt. 12 e 68 OIsFi; RS 954.11) concernenti la separazione delle funzioni, la gestione dei rischi e il controllo interno e concretizza la prassi di vigilanza in materia. Tiene conto dei Principi del Comitato di Basilea sulla sana gestione dei rischi operativi[1] e sulla resilienza operativa[2]. 1

La circolare è destinata alle banche secondo l'art. 1*a* e alle persone secondo l'art. 1*b* della Legge sulle banche (LBCR; RS 952.0), alle società di intermediazione mobiliare secondo l'art. 2 cpv. 1 lett. e e l'art. 41 della Legge sugli istituti finanziari (LIsFI; RS 954.1) nonché ai gruppi finanziari e ai conglomerati finanziari secondo l'art. 3*c* LBCR e l'art. 49 LIsFi. Di seguito le banche, le persone secondo l'art. 1*b* LBCR, le società di intermediazione mobiliare, i gruppi finanziari e i conglomerati finanziari vengono denominati congiuntamente «istituti». 2

II. Definizioni

I *rischi operativi* sono definiti nell'art. 89 dell'Ordinanza sui fondi propri (OFoP; RS 952.03). Consistono nel pericolo di incorrere in perdite finanziarie dovute all'inadeguatezza o all'inefficacia delle procedure o dei sistemi interni, all'inadeguatezza delle azioni delle persone o a errori da esse commessi oppure causate da eventi esterni. Essi comprendono le perdite finanziarie che possono insorgere da rischi legali o di *compliance*. La gestione dei rischi operativi tiene tipicamente conto anche di altre dimensioni del danno[3], nella misura in cui esse possano causare tra l'altro perdite finanziarie. Sono esclusi i rischi strategici. 3

I *rischi inerenti* sono rischi operativi a cui l'istituto è esposto a causa dei suoi prodotti, processi e sistemi e delle sue attività senza considerare le misure di controllo e di attenuazione. 4

I *rischi residui* sono rischi operativi a cui l'istituto è esposto dopo aver considerato le misure di controllo e di attenuazione. 5

Le *tecnologie dell'informazione e della comunicazione* (TIC) designano la struttura fisica e logica (elettronica) dei sistemi informatici e di comunicazione, le singoli componenti hardware e software, le reti, i dati e gli ambienti operativi. 6

I *dati critici* sono dati che, in considerazione delle dimensioni, della complessità, della struttura, del profilo di rischio e del modello commerciale dell'istituto sono importanti a tal punto da richiedere uno standard più elevato di sicurezza. Si tratta di dati essenziali ai fini dell'erogazione efficace e continuativa dei servizi dell'istituto o per scopi regolatori. Per valutare e determinare la criticità dei dati è necessario considerarne sia la confidenzialità sia l'integrità e la disponibilità. Ognuno di questi tre aspetti può essere determinante per classificare i dati come critici. 7

---

[1] *BCBS Revisions to the Principles for the Sound Management of Operational Risk* (31 marzo 2021).

[2] *BCBS Principles for Operational Resilience* (31 marzo 2021).

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

I *processi critici* sono processi la cui perturbazione importante o interruzione compromette lo svolgimento delle funzioni critiche, di cui sono parte. 8

Il *business continuity management (BCM)* designa l'approccio adottato a livello di istituto per ripristinare i processi critici in caso di perturbazione o interruzione importante che vada al di là della gestione degli incidenti. Definisce dunque la reazione a perturbazioni importanti o interruzioni. Un BCM efficace riduce i rischi residui correlati a perturbazioni importanti o interruzioni. 9

Il *recovery time objective* (RTO) è il tempo necessario per ripristinare un'applicazione, un sistema e/o un processo. Il *recovery point objective* (RPO) è la durata massima tollerabile di una perdita di dati. 10

Il *business continuity plan* (BCP) è un piano previdente che definisce le procedure, le opzioni di ripristino e le risorse sostitutive necessarie (i processi di ripristino) per garantire la continuità e il ripristino dei processi critici. 11

Il *disaster recovery plan (DRP)* definisce i processi di ripristino necessari per conseguire gli obiettivi di ripristino in caso di un guasto grave o di distruzione delle tecnologie dell'informazione e della comunicazione (TIC) e in considerazione dell'eventuale assenza di persone chiave. 12

Le *situazioni di crisi* sono situazioni straordinarie, che costituiscono una potenziale minaccia per l'esistenza e non possono essere fronteggiate con misure e competenze decisionali ordinarie. Si distinguono dagli incidenti *(incidents)* e dalle perturbazioni o dalle interruzioni importanti che possono essere fronteggiate con la gestione degli incidenti nell'esercizio normale o con i BCP e i DRP stabiliti. 13

Le *funzioni critiche* comprendono: 14

a. le attività, i processi e i servizi, incluse le risorse sottostanti necessarie al loro svolgimento, la cui interruzione pregiudicherebbe il mantenimento dell'attività dell'istituto o il suo ruolo sul mercato finanziario, quindi anche la funzionalità dei mercati finanziari; e 15

b. le funzioni di rilevanza sistemica secondo l'art. 8 LBCR. 16

La *tolleranza alle interruzioni* è la portata (p. es. durata o danni attesi) dell'interruzione di una funzione critica, che l'istituto è disposto ad accettare considerando scenari gravi, ma plausibili. Per ogni funzione critica deve essere definita una tolleranza alle interruzioni. 17

La *resilienza operativa* designa la capacità dell'istituto di ripristinare le sue funzioni critiche in caso di interruzioni entro i limiti di tolleranza alle interruzioni, ossia la capacità dell'istituto di individuare minacce e possibili disfunzioni, proteggersi da esse e reagire, ripristinare l'attività ordinaria in caso di interruzioni e trarne insegnamenti per minimizzare le conseguenze sullo svolgimento delle funzioni critiche. Un istituto operativamente resiliente ha strutturato il suo modello operativo[4] in modo tale da essere meno esposto al rischio di interruzioni in riferimento alle sue funzioni critiche. La resilienza operativa riduce quindi non solo i rischi residui delle interruzioni, ma anche il rischio inerente che si verifichino interruzioni. Una gestione efficace dei rischi operativi contribuisce a rafforzare la resilienza operativa dell'istituto. 18

[4] Spesso chiamato anche *resilience by design*.

III. Principio di proporzionalità

La presente circolare si applica fondamentalmente a tutti i suoi destinatari, tuttavia i requisiti da adempiere nel singolo caso si differenziano in funzione delle dimensioni, della complessità, della struttura e del profilo di rischio dell'istituto. Nel singolo caso, la FINMA può ordinare facilitazioni o inasprimenti. 19

Le banche e le società di intermediazione mobiliare delle categorie FINMA 4 e 5 sono esentate dall'adempimento dei numeri marginali 33–38, 41–46, 48, 51, 57, 73, 74, 76–78, 80, 87, 92, 93, 96, 103, 104 e 110–112. 20

Gli istituti di cui agli artt. 47*a*–47*e* OFoP, le persone secondo l'art. 1*b* LBCR e le società di intermediazione mobiliare che non tengono conti sono inoltre esentate dall'adempimento dei numeri marginali 72, 75, 79 e 105–109. 21

IV. Gestione dei rischi operativi

A. Gestione trasversale dei rischi operativi

La gestione dei rischi operativi rientra nella gestione del rischio a livello di istituto conformemente alla Circolare FINMA 17/1 «*Corporate governance* – banche». 22

L'organo preposto all'alta direzione approva i principi della gestione dei rischi operativi rilevanti per l'istituto e vigila sulla loro osservanza. Vi rientrano, tra l'altro, i rischi TIC, i cyber-rischi, i rischi concernenti i dati critici, i rischi derivanti dalla configurazione e dell'implementazione del BCM ed eventualmente i rischi afferenti alle prestazioni di servizio transfrontaliere. Almeno una volta all'anno approva la tolleranza al rischio per i rischi operativi conformemente alla politica di rischio in considerazione degli obiettivi strategici e finanziari dell'istituto. Al riguardo considera i risultati delle valutazioni del rischio e dei controlli secondo il nm. 30. Accetta la misura dell'esposizione ai rischi operativi da parte dell'istituto oppure decide un adeguamento della tolleranza al rischio e i necessari cambiamenti a livello strategico[5]. 23

L'organo preposto all'alta direzione approva periodicamente le strategie di gestione delle TIC, dei cyber-rischi, dei dati critici e del BCM e vigila sulla loro osservanza. 24

La direzione assicura in modo attendibile che i rischi operativi siano identificati, valutati, limitati e monitorati e che l'efficacia sia della configurazione sia dell'attuazione di tale gestione dei rischi operativi sia periodicamente verificata. Per limitare i rischi inerenti considerati essenziali[6] adotta misure integrative o inasprimenti in funzione del rischio specifico. 25

Per rendere i collaboratori sempre più consapevoli dell'importanza di ridurre i rischi operativi rilevanti, in particolare i rischi TIC, i cyber-rischi, i rischi concernenti i dati critici e i rischi derivanti dalla configurazione e dall'implementazione del BCM, è necessario implementare misure tenendo in considerazione i loro compiti, le competenze e le responsabilità (CCR)[7]. 26

[5] Per esempio un cambiamento del modello commerciale.

[6] Spesso chiamati rischi chiave *(key risks).*

[7] Ciò implica, tra l'altro, la selezione accurata e la qualificazione del personale per i CCR e la formazione continua nel quadro delle sue attività.

Se necessario, nell'ambito della vigilanza continua la FINMA definisce ulteriori requisiti in materia di gestione dei rischi operativi per temi specifici. Ciò avviene con moderazione e applicando il principio di proporzionalità. 27

I rischi operativi devono essere categorizzati secondo criteri unitari a livello di istituto e inventariati. Questa categorizzazione può essere effettuata rifacendosi alla categorizzazione utilizzata nel calcolo dei fondi propri minimi per i rischi operativi o mediante una tassonomia interna. Essa deve essere applicata in modo sistematico in tutti i settori dell'istituto e in tutte le componenti della gestione dei rischi operativi. 28

Per identificare i rischi operativi vengono considerati fattori interni[8] ed esterni[9]. I rischi operativi individuati sono valutati in modo attendibile nell'ottica sia dei rischi inerenti sia di quelli residui. 29

L'identificazione e la valutazione dei rischi operativi si basano almeno sui risultati dell'audit[10] e sulle valutazioni dei rischi e dei controlli da effettuare regolarmente. Tali valutazioni tengono conto dei rischi inerenti, dell'efficacia delle misure di controllo e di attenuazione esistenti e dei rischi residui. 30

Per valutare le misure di controllo e di attenuazione esistenti si procede in particolare a un esame regolare dell'efficacia dei controlli chiave da parte di un'istanza di controllo indipendente (*design effectiveness* e *operating effectiveness testing*), documentandone i risultati. I controlli chiave sono le misure di controllo e di attenuazione che minimizzano i rischi inerenti considerati essenziali. Anche la separazione dei CCR per garantire l'indipendenza e prevenire i conflitti di interessi è oggetto di valutazioni periodiche. 31

Prima di apportare cambiamenti sostanziali a livello di prodotti, attività, processi e sistemi è necessario effettuare valutazioni ad hoc dei rischi e dei controlli, che prendono in considerazione i rischi operativi derivanti dal processo di cambiamento e i rischi operativi delle condizioni target. Ove necessario, vengono adeguati i limiti di tolleranza al rischio e attuate misure di controllo e di attenuazione. 32

In funzione della natura, della portata, della complessità e del rischio dei prodotti, delle attività, dei processi e dei sistemi specifici all'istituto, devono essere applicati gli ulteriori strumenti e metodi seguenti: 33

a. raccolta e analisi sistematiche dei dati interni di perdita e degli eventi esterni rilevanti correlati a rischi operativi; 34

b. indicatori di rischio e di controllo per il monitoraggio dei rischi operativi e la tempestiva identificazione degli aumenti rilevanti dei rischi; 35

c. analisi di scenario e/o stima del potenziale di perdita in considerazione dei o rispetto ai fondi propri minimi per i rischi operativi; 36

[8] Sono considerati fattori interni, per esempio, i cambiamenti apportati ai prodotti, alle attività, ai processi e ai sistemi, i risultati dell'audit e le perdite interne derivanti dai rischi operativi.

[9] Sono considerati fattori esterni, per esempio, gli eventi che generano perdite in altri istituti, i cambiamenti sul piano della sicurezza (p. es. dovuti a impatti ambientali, cyber-attacchi o terrorismo) o gli adeguamenti ai requisiti normativi.

[10] In questo caso i risultati dell'audit comprendono gli esiti della revisione interna e della società di audit esterna, se disponibili, nonché i risultati delle verifiche svolte, per esempio, dalle divisioni commerciali e organizzative, dal controllo del rischio, dalla funzione preposta alla *compliance* o dalle autorità di vigilanza.

d. analisi comparative *(read-across)*, per esempio analisi della rilevanza dei risultati dell'audit in altri settori dell'istituto o confronti tra i risultati delle valutazioni del rischio e dei controlli di diversi settori. 37

La tolleranza al rischio per i rischi operativi tiene conto della tolleranza in rapporto ai rischi operativi inerenti[11] e a quelli residui ed è monitorata mediante indicatori di rischio o di controllo. 38

Il controllo dei rischi presenta all'organo preposto all'alta direzione almeno una volta all'anno e alla direzione almeno a ritmo semestrale in conformità ai nm. 75–76 della Circolare FINMA 17/1 un rapporto sui rischi operativi al massimo livello[12] della categorizzazione definita secondo il nm. 28, sul loro confronto con la tolleranza al rischio stabilita e sui dettagli concernenti le perdite interne sostanziali. 39

In riferimento ai rischi TIC e ai cyber-rischi rilevanti, il rapporto da presentare alla direzione almeno una volta all'anno contiene inoltre informazioni sull'evoluzione di tali rischi, sull'efficacia dei relativi controlli chiave e su importanti eventi interni ed esterni in relazione a tali rischi. 40

Il rapporto interno di cui al nm. 39 contiene a titolo complementare le seguenti informazioni: 41

- i fattori esterni rilevanti secondo la nota 9, 42
- una panoramica ricapitolativa sull'efficacia dei controlli chiave secondo il nm. 31, 43
- i rischi operativi emergenti, 44
- i risultati derivanti dall'applicazione degli ulteriori strumenti e metodi secondo il nm. 33. 45

Conformemente al principio di proporzionalità, per le banche di rilevanza sistemica viene presentato un resoconto periodico sui rischi operativi anche al livello delle divisioni commerciali e organizzative esposte a rischi operativi rilevanti o essenziali. 46

B. Gestione dei rischi TIC

a) Strategia TIC e *governance*

Le aspettative fondamentali poste alla strategia, alla *governance* e al rafforzamento della consapevolezza in riferimento alle TIC sono enunciate nei nm. 23–26 e 40. 47

La gestione dei rischi TIC considera standard e pratiche rilevanti riconosciuti a livello internazionale, nonché l'impatto di nuovi sviluppi tecnologici sui rischi TIC. 48

La direzione assicura, sia per la gestione del cambiamento *(change management)* sia per l'esercizio delle TIC *(run, maintenance),* l'implementazione e la documentazione di procedure, processi, controlli e CCR, a cui sono assegnate risorse qualificate e appropriate. 49

[11] La tolleranza al rischio in riferimento ai rischi inerenti considera decisioni strategiche che concernono il modello commerciale o operativo, per esempio la tolleranza per i rischi inerenti implicati dall'erogazione di servizi a determinati segmenti di clientela o Paesi, dall'offerta di determinati prodotti, dall'applicazione di processi prevalentemente manuali, dall'utilizzo di un'infrastruttura informatica complessa o da determinate esternalizzazioni *(outsourcing).*

[12] Il massimo livello della categorizzazione viene spesso chiamato livello 1 o *level 1*. Il rapporto può essere effettuato anche a un livello più dettagliato.

b) Gestione del cambiamento *(change management)*

La gestione del cambiamento definisce procedure, processi e controlli per tutte le fasi dello sviluppo o dell'acquisto di TIC e, in ognuna di queste fasi, considera l'impatto del cambiamento sui rischi TIC, focalizzandosi sui requisiti in materia di confidenzialità, integrità e disponibilità. 50

Occorre garantire una separazione tra gli ambienti di sviluppo o di test delle TIC e l'ambiente della loro produzione. Ciò comprende anche una chiara attribuzione dei CCR e la regolamentazione dei conseguenti diritti di accesso. 51

Nelle fasi di sviluppo e di acquisto delle TIC le esigenze funzionali e non funzionali[13] sono definite chiaramente e approvate, quindi testate e convalidate in funzione della loro criticità. 52

c) Esercizio delle TIC *(run, maintenance)*

L'istituto tiene uno o più inventari delle componenti TIC. L'inventario include componenti hardware e software nonché i luoghi di archiviazione di dati critici. Tiene conto delle dipendenze all'interno dell'istituto e delle interfacce con importanti fornitori esterni di servizi. 53

L'inventario, disponibile in tempi brevi, viene regolarmente verificato in termini di completezza ed esattezza e aggiornato. 54

L'istituto dispone di procedure, processi e controlli che garantiscono la confidenzialità, l'integrità e la disponibilità dell'ambiente di produzione delle TIC considerando la rispettiva tolleranza al rischio. 55

L'istituto garantisce il passaggio senza difficoltà dall'esercizio delle TIC ai suoi processi BCP e DRP in caso di perturbazioni importanti o interruzioni. Implementa opportuni processi di *backup* e di ripristino, che sono regolarmente testati e convalidati. 56

L'istituto dispone di procedure, processi e controlli che garantiscono una gestione orientata al rischio delle TIC la cui vita operativa volge al termine o che hanno superato il periodo di disattivazione previsto. 57

d) Gestione degli incidenti *(incident management)*

L'istituto dispone di procedure, processi e controlli volti a trattare incidenti TIC rilevanti, inclusi quelli riconducibili a dipendenze da importanti fornitori esterni di servizi e da esternalizzazioni in seno al gruppo. Al riguardo è necessario considerare l'intero ciclo di vita degli incidenti TIC importanti e definire i CCR per trattare questi incidenti. 58

Il trattamento degli incidenti TIC importanti deve essere coordinato e collegato ai processi BCM e DRP. 59

Gli incidenti TIC considerati dall'istituto come una perturbazione importante per lo svolgimento dei suoi processi critici e rilevanti ai fini della vigilanza devono essere notificati senza indugio alla FINMA. 60

[13] P. es. per quanto attiene all'architettura o ai requisiti di sicurezza delle informazioni.

C. Gestione dei cyber-rischi

Le aspettative fondamentali poste alla strategia, alla *governance* e al rafforzamento della consapevolezza in riferimento ai cyber-rischi sono enunciate nei nm. 23–26 e 40. 61

L'istituto definisce chiari CCR. Deve coprire almeno gli aspetti seguenti secondo standard e pratiche riconosciuti a livello internazionale e garantire, sviluppare e migliorare continuamente la loro effettiva attuazione mediante procedure, processi e controlli adeguati: 62

a. identificazione delle potenziali minacce dovute a cyber-attacchi[14] specifiche all'istituto e valutazione delle possibili conseguenze dello sfruttamento delle vulnerabilità relative alle componenti inventariate delle TIC e ai dati elettronici critici (in conformità al nm. 53, 54 e 7); 63

b. protezione delle componenti inventariate delle TIC e dei dati elettronici critici contro i cyber-attacchi mediante l'attuazione di misure di protezione adeguate, in particolare in riferimento alla confidenzialità, all'integrità e alla disponibilità; 64

c. individuazione e registrazione tempestive dei cyber-attacchi sulla base di un processo di monitoraggio sistematico e continuo delle componenti inventariate delle TIC e dei dati elettronici critici; 65

d. reazione alle vulnerabilità identificate e ai cyber-attacchi mediante lo sviluppo e l'implementazione di processi appropriati, che consentono di adottare tempestivamente misure di attenuazione e di eliminazione; e 66

e. garanzia di un rapido ripristino del normale esercizio in seguito a cyber-attacchi con misure appropriate. 67

La gestione dei cyber-rischi deve garantire che un cyber-attacco riuscito o parzialmente riuscito sia analizzato in base alla sua rilevanza per le componenti critiche inventariate delle TIC e i dati elettronici critici, nonché i processi critici (incl. i servizi e le funzioni esternalizzati) e che l'obbligo di comunicazione secondo la LFINMA sia rispettato. Dopo una prima valutazione e un'informazione preliminare al servizio competente della FINMA entro 24 ore, la comunicazione deve essere trasmessa entro 72 ore in conformità all'elenco dei requisiti della Piattaforma di rilevamento EHP (campi obbligatori). Una volta che l'istituto ha concluso la trattazione del caso, deve essere presentato al servizio competente della FINMA un rapporto conclusivo sulle cause commisurato al grado di gravità. 68

La direzione dispone regolarmente lo svolgimento di analisi di vulnerabilità[15] e test di intrusione *(penetration test)*[16], che devono essere eseguiti da personale qualificato con risorse adeguate. In proposito occorre considerare tutte le componenti inventariate delle TIC accessibili tramite internet. Inoltre, devono essere considerate le componenti inventariate delle TIC non accessibili tramite internet, ma necessarie per lo svolgimento di processi critici o contenenti dati elettronici critici. 69

[14] Attacchi alla confidenzialità, all'integrità e alla disponibilità delle TIC, nonché ai dati elettronici critici che si verificano mediante lo sfruttamento delle vulnerabilità o l'elusione delle misure di protezione da parte di aggressori esterni o interni.

[15] Analisi volta a identificare le vulnerabilità esistenti a livello di software e le falle di sicurezza nell'infrastruttura IT nei confronti di cyber-attacchi.

[16] Esame mirato e sfruttamento delle vulnerabilità a livello di software e delle falle di sicurezza nelle TIC.

Sulla base delle minacce potenziali specifiche all'istituto, devono essere svolti cyber-esercizi in funzione dei rischi e riferiti allo scenario in questione[17]. Il risultato degli esercizi deve essere documentato facendone rapporto in forma adeguata. 70

D. Gestione dei rischi dei dati critici

Le aspettative fondamentali poste alla strategia, alla *governance* e al rafforzamento della consapevolezza in riferimento ai rischi dei dati critici sono enunciate nei nm. 23–26. 71

La direzione definisce processi, procedure e controlli adeguati nonché chiari CCR concernenti la gestione dei dati critici individuati dall'istituto. Inoltre, la direzione designa un'unità preposta alla creazione di condizioni quadro che garantiscano la confidenzialità, l'integrità e la disponibilità di dati critici e al controllo del loro rispetto. 72

L'istituto individua i suoi dati critici in modo sistematico ed esaustivo, li categorizza in funzione del loro grado di criticità e definisce chiare responsabilità in materia di dati. 73

I dati critici definiti dall'istituto sono gestiti lungo il loro intero ciclo di vita. 74

Al riguardo, il rispetto della confidenzialità, dell'integrità e della disponibilità nella gestione di dati critici è garantito mediante processi, procedure e controlli adeguati. 75

Nell'esercizio e durante lo sviluppo, il cambiamento e la migrazione delle TIC, i dati critici devono essere protetti dall'accesso e dall'utilizzo da parte di soggetti non autorizzati. Questo vale anche per i dati critici in ambienti di test. 76

In particolare devono essere protette le componenti delle TIC in cui sono archiviati o trattati dati critici. È necessario regolamentare sistematicamente e monitorare continuamente l'accesso a questi dati. 77

L'accesso ai dati critici e alle funzioni legate al trattamento di questi dati è limitato alle persone che necessitano dei dati per svolgere i propri compiti[18]. Al riguardo l'istituto deve disporre di un sistema di autorizzazione. L'accesso a tale sistema di autorizzazione deve essere protetto in modo particolare e verificato regolarmente. Le autorizzazioni contenute nel sistema devono essere verificate regolarmente. 78

Se i dati critici sono archiviati al di fuori della Svizzera[19] o sono accessibili dall'estero, è necessario limitare adeguatamente i rischi superiori che ne derivano e monitorarli mediante misure adeguate, nonché proteggere i dati in modo particolare. 79

Occorre scegliere accuratamente le persone interne e quelle esterne che possono accedere ai dati critici o modificarli. Tali persone devono essere sorvegliate mediante misure appropriate[20] e formate regolarmente sulla gestione di questi dati. Alle persone che beneficiano di maggiori privilegi[21] si applicano requisiti di sicurezza più rigorosi. Inoltre, deve essere tenuto un elenco di tutte le persone che beneficiano di maggiori privilegi e aggiornato continuamente. 80

[17] Considerando il nm. 19, questi cyber-esercizi potrebbero includere, per esempio, esercizi di simulazione *(table-top exercises)*, *red teaming* ecc.

[18] P. es. principio del *need-to-know* e del privilegio minimo *(least privilege).*

[19] P. es. mediante soluzioni di *cloud* o di *hosting.*

[20] P. es. valutazione di file log, principio del doppio controllo ecc.

[21] P. es. persone con diritti di amministratore, utenti con accesso funzionale a una grossa quantità di dati critici ecc.

Gli incidenti che compromettono in misura significativa la confidenzialità, l'integrità o la disponibilità di dati critici devono essere notificati senza indugio alla FINMA. 81

Nella scelta dei fornitori di servizi che trattano dati critici[22] o possono consultarli deve essere attribuita una notevole importanza alla verifica della diligenza *(due diligence).* Occorre definire criteri chiari per valutare il modo in cui i fornitori di servizi gestiscono dati critici ed esaminarlo prima di firmare i contratti. I fornitori di servizi devono essere sottoposti a un monitoraggio e a un controllo periodici nell'ambito del sistema di controllo interno dell'istituto. 82

E. *Business continuity management* (BCM)

Le aspettative fondamentali poste alla strategia, alla *governance* e al rafforzamento della consapevolezza in riferimento ai rischi che derivano dalla configurazione e dall'implementazione del BCM sono enunciate nei nm. 23–26. 83

Ogni divisione operativa e organizzativa rilevante deve individuare i suoi processi critici e le risorse necessarie[23] nell'ambito della *business impact analysis* (BIA). 84

Per i processi critici, l'istituto definisce il RTO e il RPO secondo il nm. 10, coordinandoli con i necessari fornitori di servizi[24]. La loro osservanza è disciplinata mediante *service level agreement* o contratti, oppure è garantita mediante procedure, processi e controlli appropriati. 85

L'istituto definisce almeno un BCP secondo il nm. 11, che descrive anche gli eventi che comportano l'attivazione del piano e i processi decisionali e tiene conto della perdita di risorse secondo il nm. 84. I rischi residui accettati sono documentati in maniera adeguata. 86

La BIA e il BCP sono allestiti e documentati in modo sistematico secondo una direttiva applicabile a tutto l'istituto. Devono essere verificati e aggiornati ogni anno e ad hoc in caso di cambiamenti sostanziali nell'attività (riorganizzazioni, creazione di un nuovo campo di attività ecc.). 87

L'istituto definisce almeno un DRP come parte integrante del BCP. Se vengono esternalizzati processi critici o singole parti di essi, il DRP tiene conto delle dipendenze interne e delle disposizioni contrattuali nonché di soluzioni alternative. Il DRP è verificato e aggiornato ad hoc in caso di cambiamenti sostanziali, ma almeno una volta all'anno. 88

Nelle situazioni di crisi, uno stato maggiore di crisi è incaricato di gestire la crisi fino al ripristino della situazione conforme. Gli eventi che scatenano una crisi e i CCR dello stato maggiore di crisi devono essere previamente regolamentati e l'organizzazione di crisi deve essere incentrata sull'attività commerciale e la struttura geografica dell'istituto. Nelle situazioni di crisi deve essere garantita la reperibilità dei responsabili. 89

L'istituto definisce una strategia di comunicazione interna ed esterna nelle situazioni di crisi. 90

---

[22] Trattamento: qualunque modo di gestire dati critici, a prescindere dai mezzi e dalle procedure impiegati, in particolare l'acquisizione, il salvataggio, la custodia, l'utilizzo, la modifica, la divulgazione, l'archiviazione, la cancellazione o l'eliminazione dei dati.

[23] Personale, infrastrutture (p. es. immobili, infrastruttura dei posti di lavoro), informazioni, sistemi IT o infrastruttura IT (compresi i sistemi di comunicazione), dipendenze da altri settori dell'istituto e da terzi, p. es. erogatori di servizi e fornitori esterni *(outsourcing),* banche centrali o stanze di compensazione.

[24] P. es. con la sezione IT, altre divisioni dell'istituto o esterni.

L’attuazione del BCP e del DRP e la funzionalità dell’organizzazione di crisi sono regolarmente valutate. A tal fine l’istituto appronta una pianificazione sistematica dei test che garantisce la copertura regolare. È possibile scegliere diverse modalità di test con gradi di intensità e di efficacia variabile, per esempio gli esercizi *table-top.* 91

Le principali misure in conformità al BCP e al DRP e l’organizzazione di crisi sono testate almeno una volta all’anno. 92

I principali *stakeholder*, compresi quelli che svolgono funzioni specialistiche e IT, partecipano ai test per acquisire dimestichezza con i processi di ripristino. 93

I test comprendono scenari di diversa gravità, ma plausibili e considerano le dipendenze ai fini del ripristino, comprese quelle nei confronti di terzi interni o esterni. 94

Resoconti periodici all’organo preposto all’alta direzione e alla direzione informano in merito alle attività di test e di verifica condotte e ai relativi risultati. Presentano chiaramente le priorità adottate (p. es. gerarchia delle priorità dei processi critici necessari per l’esecuzione delle funzioni critiche secondo il nm. 14) e le lacune individuate nella copertura di altri processi critici. 95

I collaboratori e i membri dell’organizzazione di crisi sono adeguatamente preparati riguardo ai loro CCR riconducibili alle diverse attività di BCM sia al momento dell’entrata in servizio sia nel corso delle formazioni periodiche. 96

F. Gestione dei rischi afferenti alle prestazioni di servizio transfrontaliere

Se gli istituti o le società del gruppo forniscono servizi o distribuiscono prodotti finanziari oltrefrontiera, anche i rischi risultanti dall’applicazione delle normative estere (diritto fiscale, penale, in materia di riciclaggio di denaro ecc.) devono essere adeguatamente rilevati, limitati e controllati. 97

Gli istituti sottopongono le loro prestazioni di servizio transfrontaliere e la distribuzione transfrontaliera di prodotti finanziari a un’analisi approfondita delle condizioni quadro giuridiche e dei rischi correlati. Sulla base di questa analisi, gli istituti adottano le necessarie misure strategiche e organizzative volte a eliminare e minimizzare i rischi e le adeguano continuamente all’evolversi della situazione. In particolare dispongono delle necessarie competenze specialistiche specifiche ai vari Paesi, definiscono specifici modelli di servizi per i Paesi in cui li erogano, formano i collaboratori e garantiscono l’osservanza delle prescrizioni mediante misure organizzative, direttive, modelli retributivi e sanzionatori. 98

È necessario considerare anche i rischi generati da gestori patrimoniali indipendenti, intermediari e altri fornitori di servizi. I partner devono essere scelti e formati con l’opportuna accuratezza. 99

Questo principio si applica pure alle situazioni in cui una filiale, una succursale o un’entità simile con sede all’estero di un istituto finanziario svizzero fornisce servizi transfrontalieri ai clienti. 100

V. Garanzia della resilienza operativa

L’istituto identifica le sue funzioni critiche e i rispettivi limiti di tolleranza alle interruzioni, che sono approvati dall’organo preposto all’alta direzione. Inoltre, l’organo preposto 101

all'alta direzione approva e sorveglia regolarmente la procedura volta a garantire la resilienza operativa.

L'istituto adotta misure per garantire la resilienza operativa considerando scenari gravi, ma plausibili[25]. 102

Le funzioni critiche e i correlati limiti di tolleranza alle interruzioni secondo il nm. 14 devono essere approvati dall'organo preposto all'alta direzione almeno una volta all'anno. 103

L'istituto coordina le principali componenti di una gestione completa del rischio, per esempio la gestione dei rischi operativi, inclusa la gestione del rischi TIC e dei cyber-rischi, il *business continuity management*, la gestione delle esternalizzazioni (*outsourcing*; cfr. Circ. FINMA 18/3 «*Outsourcing*») e la pianificazione d'emergenza (capitolo VI), affinché contribuiscano a rafforzare la resilienza operativa dell'istituto. Ciò include uno scambio adeguato delle informazioni rilevanti tra i diversi ambiti. 104

L'organo preposto all'alta direzione e la direzione devono ricevere almeno una volta all'anno un resoconto sulla resilienza operativa, nonché in caso di lacune sostanziali nei controlli o di incidenti che compromettono la resilienza operativa. 105

Per le funzioni critiche si procede a identificare e valutare le minacce interne ed esterne come pure lo sfruttamento delle vulnerabilità. I risultanti rischi operativi sono identificati, valutati, limitati e monitorati nell'ambito della loro gestione. 106

L'istituto tiene un inventario delle sue funzioni critiche da verificare e aggiornare almeno una volta all'anno. Tale inventario contiene le tolleranze alle interruzioni delle funzioni critiche, nonché i collegamenti e le dipendenze tra i processi critici necessari e le relative risorse[26] per svolgere le funzioni critiche. 107

Per le funzioni critiche sono documentati almeno i rischi operativi essenziali e i controlli chiave. 108

Le funzioni critiche nonché le risorse e i processi critici necessari alla loro esecuzione sono coperti dai BCP secondo il capitolo IV. lettera e. 109

La capacità di eseguire funzioni critiche entro i loro limiti di tolleranza alle interruzioni in scenari gravi, ma plausibili è regolarmente testata o esercitata. Ciò comprende anche gli scenari che si differenziano dalle interruzioni brevi e con un effetto piuttosto limitato e sono caratterizzati da una durata prolungata (p. es. diversi mesi) e dall'insufficienza delle risorse fondamentali[27]. I test e gli esercizi sono configurati in modo tale da non costituire una minaccia sostanziale per l'istituto. 110

Per le banche di rilevanza sistemica, il BCP, il DRP e l'organizzazione di crisi in conformità al capitolo IV. lett. E., rilevanti per il mantenimento delle funzioni critiche secondo il nm. 14, devono essere coordinati con la pianificazione d'emergenza in conformità al capitolo VI. 111

[25] Non si può escludere che alcuni scenari non possano essere fronteggiati senza il coinvolgimento dello Stato (p. es. pandemie, guerre, persistente penuria di energia). In tali casi l'istituto deve svolgere lavori preliminari volti a rafforzare la sua resilienza operativa nei confronti di questi scenari nell'ambito delle sue possibilità.

[26] Incluse le componenti dell'inventario rilevanti per le funzioni critiche secondo il nm. 53.

[27] Tra gli altri, una pandemia, una penuria di energia, un'insufficienza prolungata ascrivibile all'insolvenza di un importante fornitore di servizi (p. es. con conseguente ritiro da un accordo di *outsourcing*) o un divieto prolungato da parte di governi stranieri, in base al quale i fornitori di servizi *cloud* o altri fornitori di servizi con sede all'estero non sono più autorizzati a erogare servizi alle società svizzere.

VI. Mantenimento dei servizi critici in caso di liquidazione o risanamento delle banche di rilevanza sistemica

Nel quadro della loro pianificazione d'emergenza, le banche di rilevanza sistemica adottano le misure necessarie per garantire il mantenimento senza interruzioni delle funzioni di rilevanza sistemica (art. 9 cpv. 2 lett. d LBCR in combinato disposto con l'art. 60 segg. OBCR). Identificano i servizi essenziali per il mantenimento delle funzioni di rilevanza sistemica in caso di liquidazione, risanamento o ristrutturazione («servizi critici») e adottano le misure necessarie a tale scopo. Al riguardo tengono conto delle disposizioni emanate in materia dagli organismi internazionali di standardizzazione. 112

VII. Disposizioni transitorie

A. Concernenti la garanzia della resilienza operativa

L'identificazione delle funzioni critiche, la definizione della tolleranza alle interruzioni e le prime approvazioni in conformità ai nm. 101 e 103, nonché un primo resoconto secondo il nm. 105 sono attesi a partire dall'entrata in vigore della presente circolare. Per l'adempimento dei requisiti di cui ai nm. 106–109 e i primi test secondo il nm. 110 è accordato un termine transitorio di un anno dall'entrata in vigore. La garanzia della resilienza operativa in conformità al nm. 102 e l'adempimento dei requisiti di cui ai nm. 104 e 111 sono attesi entro un termine transitorio di due anni. 113

B. Concernenti le esigenze in materia di fondi propri per la copertura dei rischi operativi

Le esigenze in materia di fondi propri per i rischi operativi ai sensi degli artt. 89 segg. OFoP sono rette dai nm. 3–116 della Circolare FINMA 08/21 «Rischi operativi – banche» sino all'entrata in vigore dell'OFoP riveduta nel quadro del pacchetto di revisioni «Basilea III finale» e della relativa ordinanza esecutiva della FINMA. 114

Allegato 1

Grafico esplicativo sulla resilienza operativa

Componenti per lo svolgimento della funzione critica