Risultati dei controlli in loco

Simposio per le piccole banche – 7 settembre 2026

Programma

1

Panoramica dei controlli in loco

- Vigilanza orientata al rischio
- Differenze fra gli strumenti di vigilanza
- Principio di proporzionalità
- Statistiche
- Rischi elevati e molto elevati

2

Temi centrali

- Riciclaggio di denaro – e finanziamento del terrorismo
- Ipoteche
- Cyber

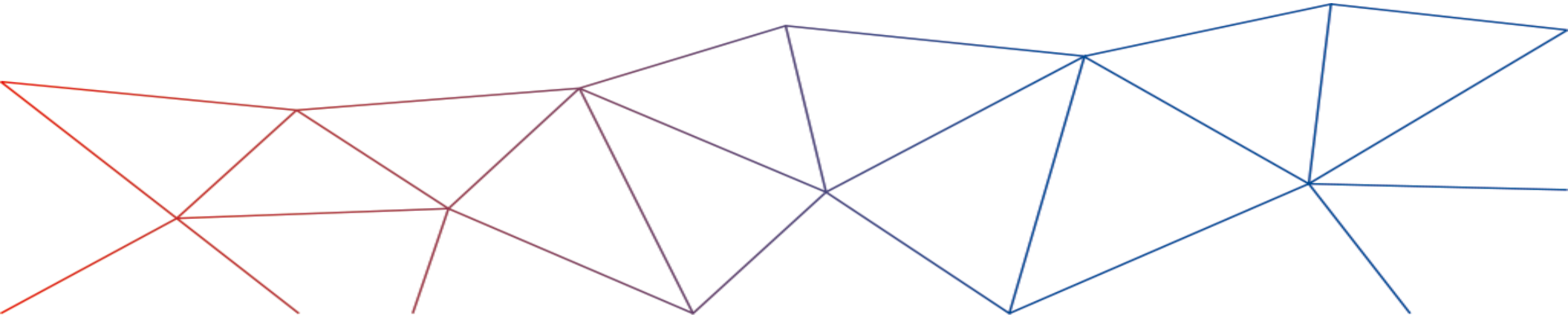
3

Conclusione

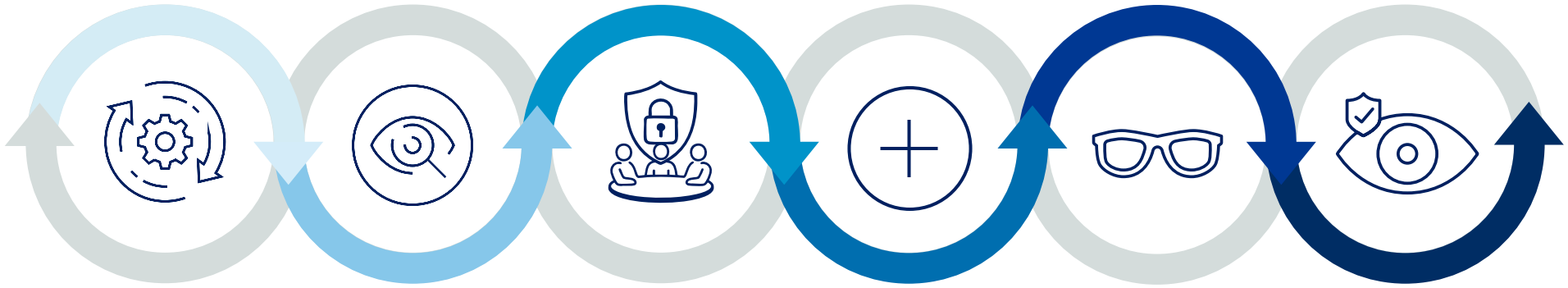
- Domande

Panoramica dei controlli in loco

Banche e società di intermediazione mobiliare



Vigilanza orientata al rischio



Variazione della situazione di rischio

Utilizzo degli strumenti di vigilanza orientato al rischio, inclusi i controlli in loco

Maggiore intensità delle verifiche e verifiche approfondite

Constatazioni identificate a più riprese

Maggiore trasparenza

Nuova valutazione della situazione di rischio

La vigilanza orientata al rischio, con un ambito di verifica più ampio, consente una maggiore trasparenza sui rischi esistenti.

Differenze fra gli strumenti di vigilanza

	Strumenti di vigilanza indiretti: fra le altre cose, audit prudenziale da parte delle società di audit	Strumenti di vigilanza diretti: fra le altre cose, controlli in loco
Quadro dell'audit	Audit di ambiti di verifica prudenziali definiti	Verifica flessibile e approfondita di determinati temi di vigilanza e di rischio
Portata e ampiezza	Ampiezza dell'audit standardizzata e orientata al rischio secondo le disposizioni della FINMA	Determinazione flessibile e orientata al rischio dell'ampiezza dell'audit
Procedura	Da parte della società di audit secondo standard di verifica stabiliti	Selezione commisurata alle esigenze di atti di vigilanza e di verifica adeguati
Valutazione	Attestazione di audit indipendente e rendiconto alla FINMA	Propria valutazione del rischio prudenziale della FINMA
Risultato	**Rapporto di audit con irregolarità e raccomandazioni**	**Constatazioni prudenziali ed eventualmente misure della FINMA**

Basi

Legge sulla vigilanza dei mercati finanziari (LFINMA) art. 24 segg., in particolare artt. 27 e 29 e art. 31 segg.
Ordinanza sugli audit dei mercati finanziari (OA-FINMA) e Ordinanza della FINMA sull'audit prudenziale
Circolare FINMA 25/1 «Attività di audit»

Principio di proporzionalità

Numero di controlli in loco	2023		2024		2025	
	Totale	Ø per istituto	Totale	Ø per istituto	Totale	Ø pro Institut
Cat. 1	33	**33**	45	**45**	47	**47**
Cat. 2	10	**3,3**	15	**5,0**	14	**4,7**
Cat. 3	34	**1,2**	34	**1,3**	35	**1,3**
Cat. 4	10	**0,2**	6	**0,1**	11	**0,2**
Cat. 5	7	**0,05**	10	**0,06**	10	**0,06**
n/a*	0	**n/a**	1	**n/a**	1	**n/a**

** Controlli in loco presso fornitori esterni*

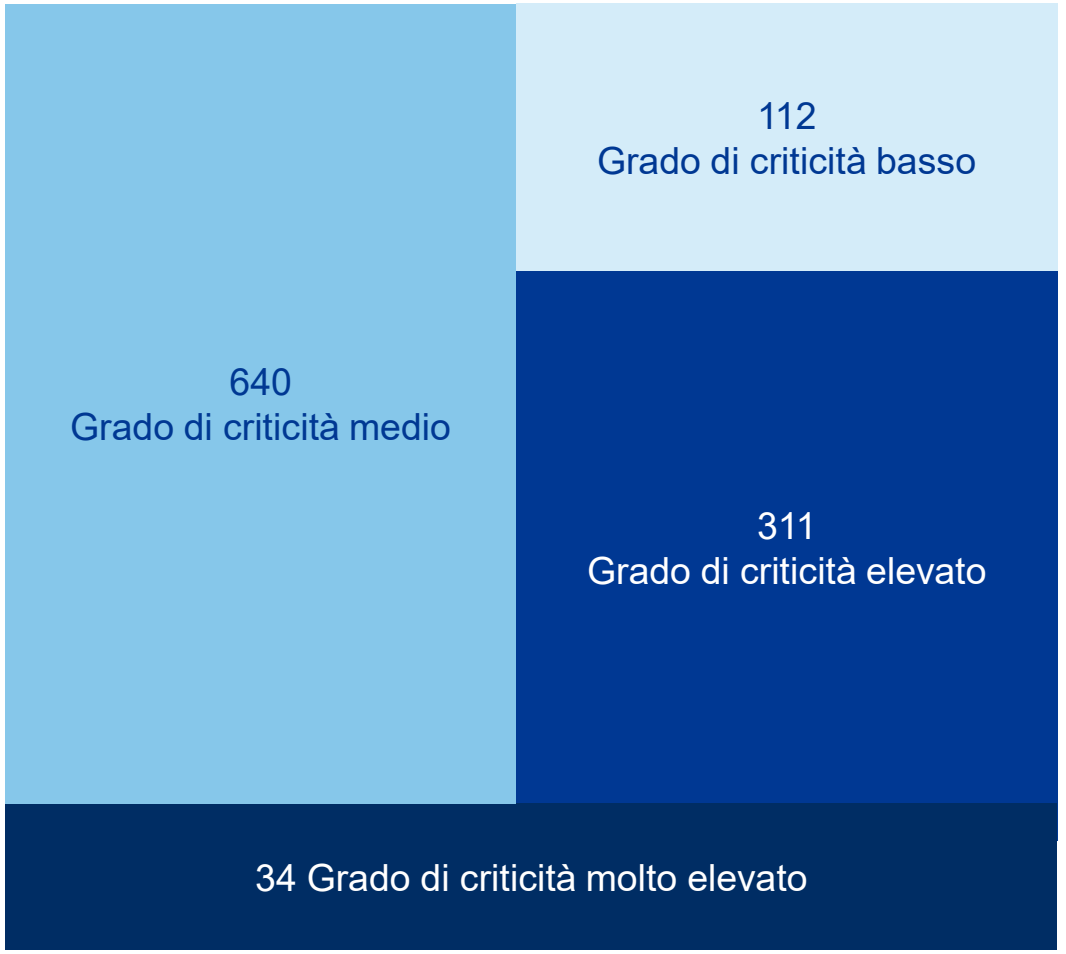
Statistiche

3 anni (2023-2025)

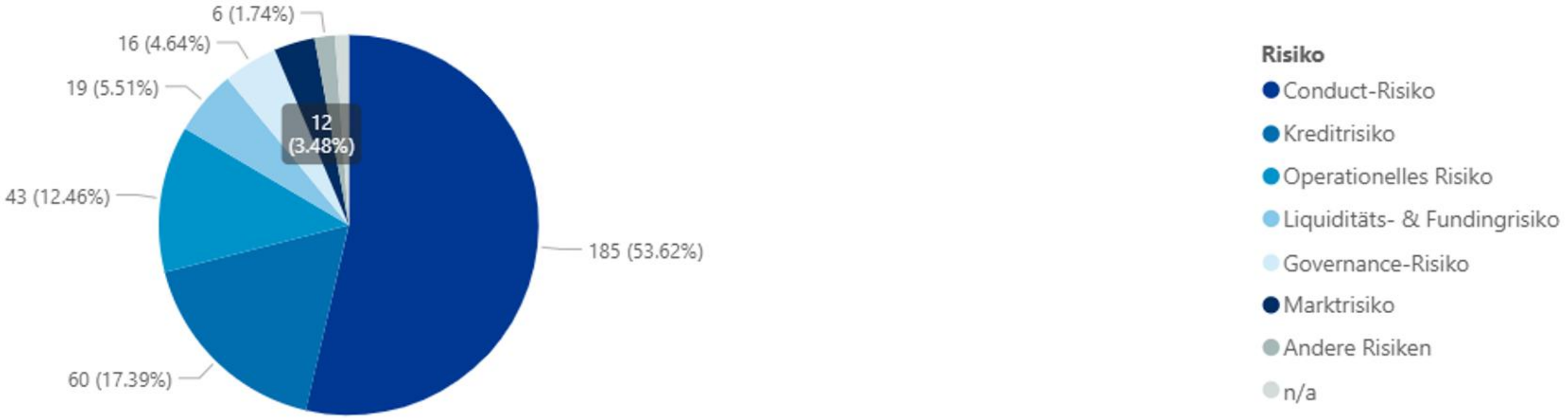
71 istituti (categoria 2-5)

198 controlli in loco

1097 constatazioni

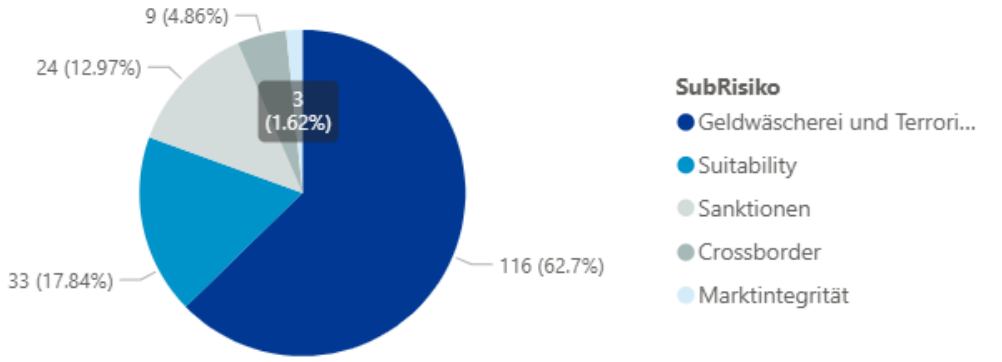


Constatazioni con rischi elevati e molto elevati – visione d'insieme

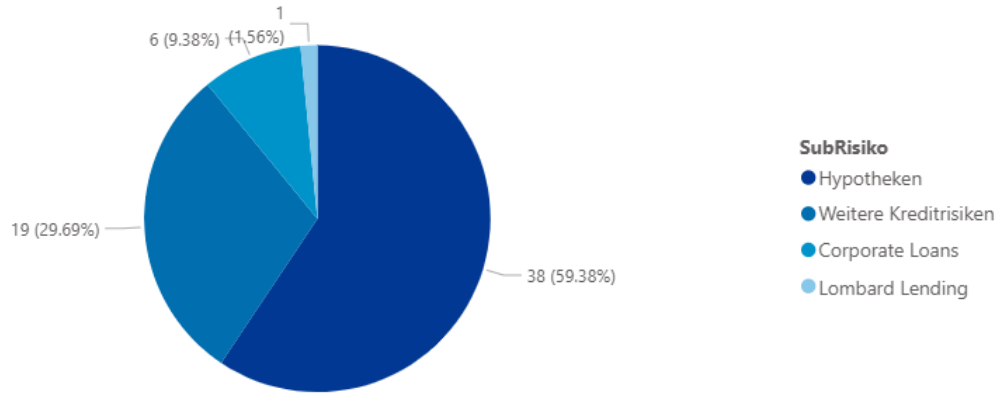


Constatazioni con rischi elevati e molto elevati – temi principali

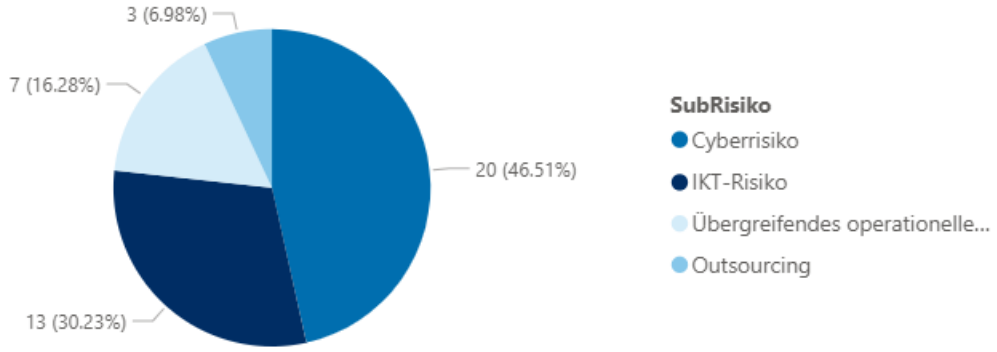
Rischio *conduct*



Rischio di credito

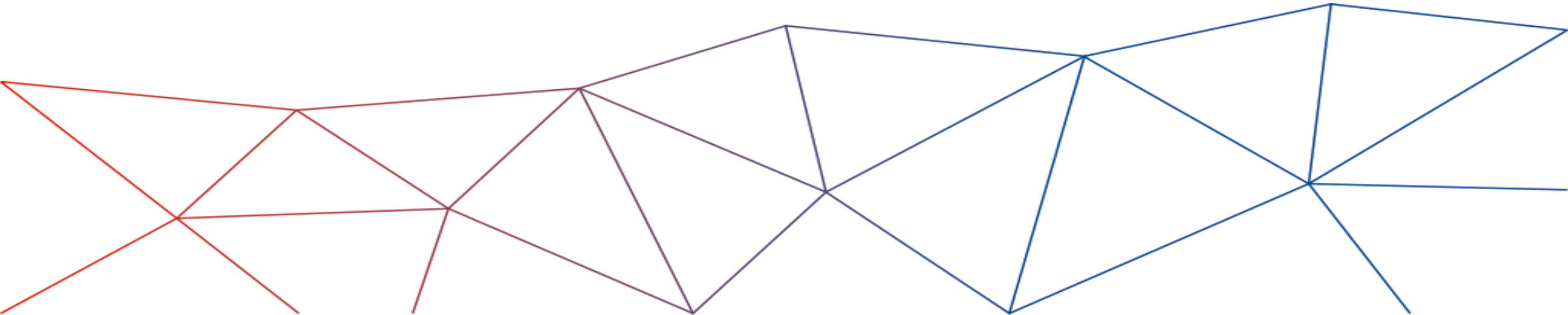


Rischio operativo



Tema centrale

Riciclaggio di denaro – e finanziamento del terrorismo (LRD)



Principi generali – Aspettative della FINMA in materia di vigilanza sul tema “LRD”

Tolleranza al rischio

Un efficace dispositivo di lotta contro il riciclaggio di denaro presuppone una tolleranza al rischio chiaramente definita dall’organo preposto all’alta direzione dell’intermediario finanziario *(tone from the top)*. Devono essere esclusi determinati segmenti di clientela e servizi a rischio elevato.

Comunicazione e cooperazione

I fatti sospetti devono essere comunicati senza indugio all’Ufficio di comunicazione in materia di riciclaggio di denaro (MROS). Gli istituti cooperano in maniera adeguata con le autorità.

Approccio orientato al rischio

Gli istituti applicano un approccio orientato al rischio per identificare, valutare, gestire e monitorare i loro rischi di riciclaggio di denaro e finanziamento del terrorismo. Le misure sono in linea con il profilo di rischio.

Formazione e sensibilizzazione

I collaboratori devono essere formati in maniera regolare e adeguata. Gli istituti promuovono una cultura di integrità e sensibilizzazione ai rischi di riciclaggio di denaro e finanziamento del terrorismo.

Clienti e partner commerciali

Gli istituti attuano adeguati obblighi di diligenza, conoscono i loro clienti e partner commerciali e comprendono lo scopo e il tipo di relazione d’affari.

Controllo e sicurezza

Controlli interni adeguati, verifiche indipendenti e verifiche regolari dell’efficacia garantiscono l’efficacia e l’adeguatezza delle misure.

Monitoraggio delle transazioni

Gli istituti monitorano in modo continuo le relazioni d’affari e le transazioni, per individuare e chiarire attività inusuali o sospette.

Documentazione

Gli istituti documentano in modo completo, chiaro e aggiornato i loro rischi di riciclaggio di denaro e finanziamento del terrorismo, le loro misure e decisioni e i loro controlli.

Base

Tali principi si basano sulla Legge sul riciclaggio di denaro (LRD), sull’Ordinanza sul riciclaggio di denaro (ORD) e sulle Circolari della FINMA.

Constatazioni della FINMA sul tema “LRD”

Anzahl VOK[1]

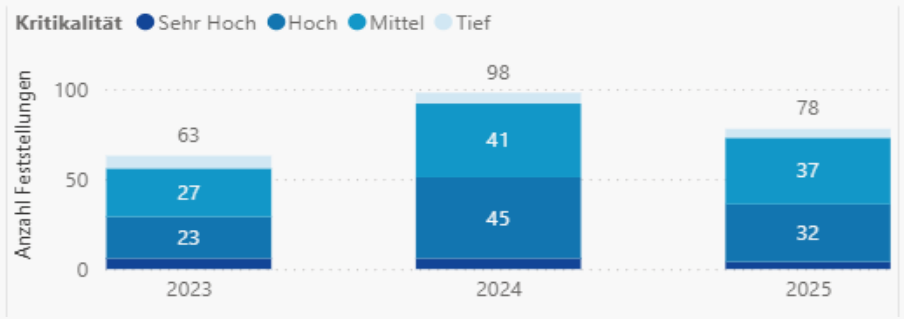
im Zeitraum

33

Ø Anzahl Feststellungen

pro VOK

7.24



Documentazione KYC

- Ripetute carenze relativamente a relazioni d’affari *cross-booking*
- Ritardi nella verifica periodica delle relazioni d’affari

Riconoscimento di transazioni che comportano un rischio superiore

- Riconoscimento esclusivamente di cosiddetti "AML hits", che non si basano sulla definizione di transazioni che comportano un rischio superiore secondo l’art. 14 ORD-FINMA
- Transazioni su conti di passaggio considerate solo in caso di pagamento o versamenti in contanti; le transazioni su conti di passaggio non effettuate in contanti non vengono rilevate dal sistema.

Tolleranza al rischio

- Elevata tolleranza al rischio concernente clienti con elevati rischi di reputazione (p. es. clienti coinvolti in controversie giuridiche di grande risonanza mediatica, che operano in settori di attività sensibili o hanno un legame con autocrati).

1 Numero di controlli in loco con constatazioni sul tema centrale

Rischi centrali in ambito LRD

Gestione patrimoniale

In particolare nell'ambito della gestione patrimoniale si continuano a osservare rischi elevati che non possono essere adeguatamente monitorati e limitati mediante il dispositivo di lotta LRD. Le persone politicamente esposte (p. es. pubblici ufficiali o responsabili in seno a imprese statali o parastatali) da Paesi a rischio elevato comportano, come clientela, rischi di riciclaggio di denaro nonché rischi giuridici e di reputazione particolarmente elevati per gli intermediari finanziari.

Retail banking

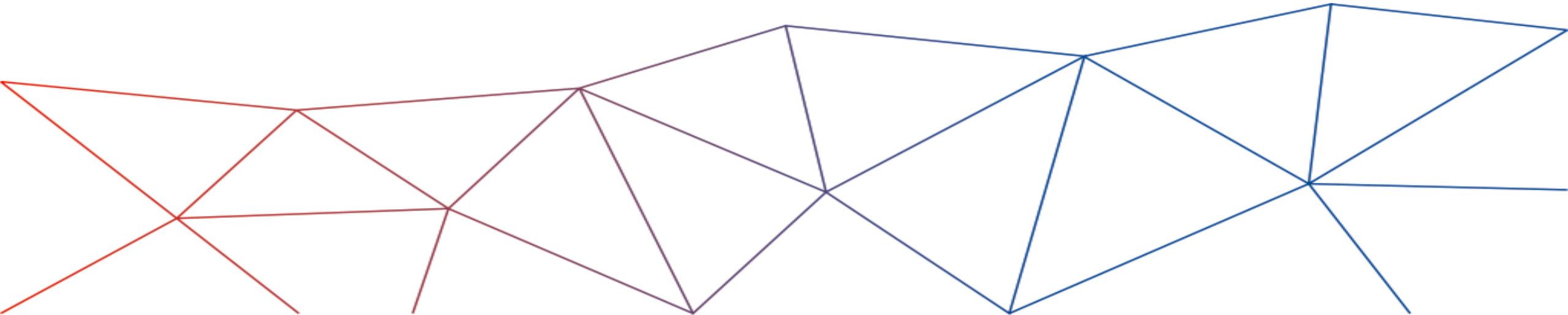
Carenze nella combinazione di criteri e scenari statici e dinamici nel monitoraggio delle transazioni portano, da un lato, a non riconoscere le transazioni sospette e, dall'altro, a un numero elevato di allerte false positive. In particolare nelle transazioni in contanti vi è il rischio che manchino gli scenari per il relativo monitoraggio o che siano inadatti a riconoscere le transazioni sospette in contanti o su conti di passaggio.

Cripto

In ambito cripto i rischi di riciclaggio di denaro sono elevati. Spesso le criptovalute vengono utilizzate come mezzo di pagamento nei cyber-attacchi, nel commercio online illegale o per eludere le sanzioni.

Tema centrale

Ipoteche



Principi generali – Aspettative della FINMA in materia di vigilanza sul tema “Ipoteche”

Solida concessione creditizia

Le ipoteche vengono concesse solo a clienti in buone condizioni di solvibilità. La sostenibilità viene accuratamente verificata e adeguatamente documentata.

Documentazione

Decisioni in merito al credito, calcoli sulla sostenibilità, anticipi e garanzie devono essere documentati in modo completo, chiaro e aggiornato.

Anticipo adeguato

L’anticipo corrisponde alle disposizioni normative. I fondi propri ed eventuali garanzie supplementari vengono considerati in maniera adeguata.

Processi e competenze

Chiari processi, competenze e controlli garantiscono un’applicazione uniforme. I collaboratori dispongono delle competenze necessarie.

Valutazione orientata al rischio e determinazione dei prezzi

La valutazione dei rischi di credito è orientata al rischio. Essa confluisce nella determinazione dei prezzi, come pure nelle decisioni relative al credito e nelle condizioni imposte.

Gestione dei rischi legati al mercato e al valore degli immobili

I rischi legati al mercato e al valore degli immobili vengono considerati in maniera adeguata. Le valutazioni devono essere verificate in modo conservativo, plausibile e regolare.

Monitoraggio e individuazione precoce

Gli istituti monitorano in modo continuo i portafogli ipotecari e individuano precocemente i rischi. All’occorrenza vengono adottate misure adeguate.

Prevenzione dei conflitti d’interesse

I conflitti d’interesse vengono individuati, evitati e, laddove inevitabili, resi trasparenti e gestiti in modo adeguato.

Base

Tali principi si basano sulla Legge sulle banche (LBCR), sull’Ordinanza sulle banche (OBCR) , nonché sulle Circolari della FINMA e sulle Comunicazioni FINMA sulla vigilanza.

Constatazioni della FINMA sul tema “Ipoteche”

Anzahl VOK [1]

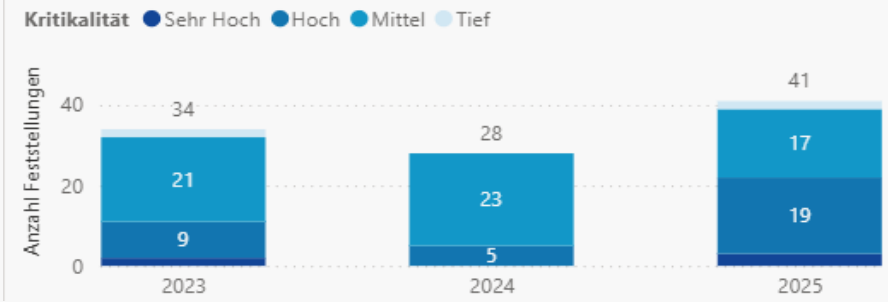
im Zeitraum

18

Ø Anzahl Feststellungen

pro VOK

5.72



Organizzazione delle funzioni di controllo e SCI

- Mancanza di un controllo indipendente delle decisioni relative al credito prese dalle unità di front office
- Mancanza di controlli indipendenti delle valutazioni immobiliari effettuate (tramite front o periti immobiliari)

Valutazione immobiliare e relativi controlli

- Mancanza di requisiti in materia di qualifica ed esperienza per i collaboratori del front office che effettuano valutazioni immobiliari
- Garanzia insufficiente dell’indipendenza delle valutazioni immobiliari

Valutazione della sostenibilità

- Criteri di sostenibilità non sostenibili
- Reporting insufficiente in materia di EtP e mancanza di una base di dati per un monitoraggio coerente dell’evoluzione delle EtP sull’arco di vari trimestri

1 Numero di controlli in loco con constatazioni sul tema centrale

Differenze a seconda della categoria di vigilanza sul tema “Ipoteche”

L’enfasi prudenziale negli ambiti di ipoteche e strumenti di vigilanza impiegati è sostanzialmente la stessa in tutte le categorie di vigilanza. Le differenze riguardano principalmente l’intensità, la portata e la frequenza della vigilanza orientata al rischio, tenendo conto di **dimensioni**, **modello operativo** e **profilo di rischio** dell’istituto.

Focus dell’attività di vigilanza

- Gestione del rischio e *governance*
- Concessione creditizia e direttive in materia di credito
- Monitoraggio dei crediti e sistema di controllo interno
- Valutazione e garanzie
- *Recovery* e rettifiche di valore
- Ordinanza sui fondi propri

Strumenti di vigilanza impiegati

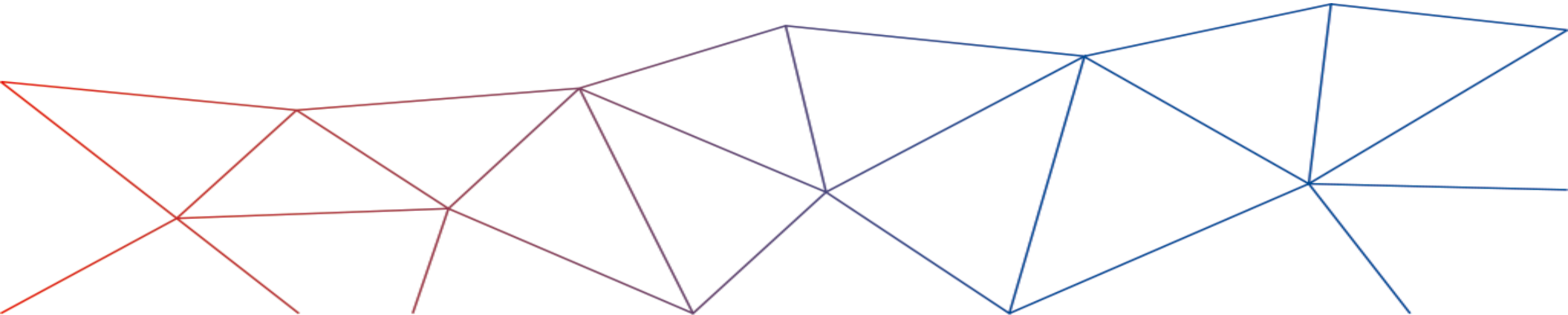
- Controlli in loco / *deep dive*
- Dialogo in materia di vigilanza
- *Reporting* / analisi dei dati / sondaggi EHP
- Analisi dei rapporti di audit
- *Stress test* e analisi

Temi critici

- Quote di EtP elevate
- Criteri di sostenibilità
- Mercato immobiliare e andamento dei tassi d’interesse

Tema centrale

Cyber



Principi generali – Aspettative della FINMA in materia di vigilanza sul tema “Cyber”

Governance e responsabilità

Il Consiglio di amministrazione e la Direzione si assumono la responsabilità generale per la cyber-resilienza. I ruoli, le responsabilità e le competenze sono chiaramente definite e organizzate in maniera adeguata.

Individuazione e reazione

I cyber-incidenti vengono precocemente individuati, gestiti in modo strutturato e notificati. Gli istituti dispongono di processi efficaci di reazione ed *escalation* e collaborano con le autorità.

Gestione del rischio

Gli istituti identificano, valutano e gestiscono in modo sistematico i cyber-rischi. Le misure sono orientate al rischio e integrate nella gestione del rischio complessivo.

Parti terze e catene di fornitura

I cyber-rischi derivanti da esternalizzazioni e parti terze vengono gestiti adeguatamente. Contratti, monitoraggio e strategie di *exit* garantiscono un controllo costante.

Garanzia tecnica e organizzativa

Gli istituti implementano adeguate misure tecniche ed organizzative per garantire la confidenzialità, l’integrità, la disponibilità e l’autenticità.

Test e resilienza

Test regolari (p. es. *vulnerability scan*, *penetration test*, esercizi *tabletop*) verificano l’efficacia delle misure e rafforzano la resilienza.

Dati e identità

La protezione dei dati e delle identità è garantita. L’accesso è effettuato in base al principio dei diritti minimi *(least privilege)*. La sicurezza dei dati e il relativo ripristino sono garantiti.

Monitoraggio e miglioramento continuo

I cyber-rischi e le misure di controllo vengono costantemente monitorate e migliorate. Si tiene conto in maniera sistematica dei risultati dei casi concreti e delle modifiche.

Base

Questi principi si basano sulla Circolare FINMA 23/1 «Rischi operativi – banche» e sulle aspettative della FINMA in materia di vigilanza.

Constatazioni della FINMA sul tema “Cyber”

1

Anzahl VOK

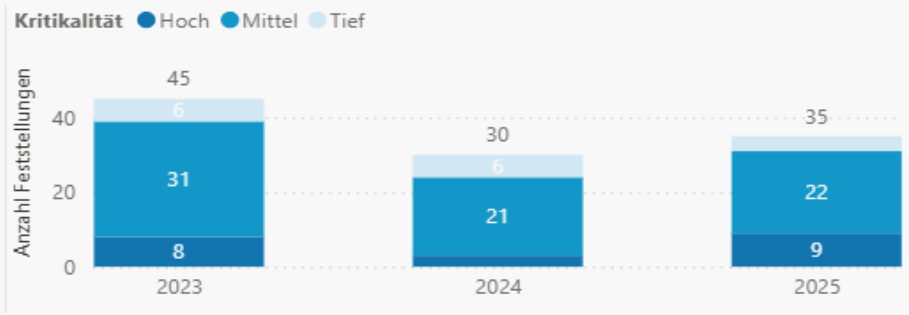
im Zeitraum

16

Ø Anzahl Feststellungen

pro VOK

6.88



Gestione del rischio

– Assenza di una definizione a sé stante di cyber-rischi
– Elevata tolleranza al rischio per furto critico di dati, perdita di dati o violazione della protezione dei dati

Analisi delle vulnerabilità e *penetration test*

– Mancanza di analisi delle vulnerabilità della rete interna
– Mancanza di una strategia e disposizioni insufficienti per lo svolgimento di *penetration test*
– Rispetto insufficiente della regolarità prevista dalla Circ. FINMA 23/1 nello svolgimento di analisi delle vulnerabilità e *penetration test*.

Capacità di reazione

– Insufficiente reattività tempestiva
– Sviluppo e implementazione insufficiente dei processi volti a far fronte alle vulnerabilità informatiche

1 Numero di controlli in loco con constatazioni sul tema centrale

Differenze a seconda della categoria di vigilanza sul tema “Cyber”

Banche cat. 2-3

Focus dell’attività di vigilanza

- Cyber-esercizi basati su scenari (c.d. *red teaming* per la cat. 2)
- Integrazione dei cyber-rischi nella gestione dei rischi operativi
- Operazionalizzazione e integrazione di un *cyber threat landscape* nel *reporting* al *management*

Strumenti di vigilanza impiegati

- Svolgimento di controlli in loco
- Tematizzazione dei cyber-rischi nei colloqui di vigilanza
- Comunicazione in ambito cyber e considerazione di *third party provider*

Temi critici

- Inventariazione insufficiente di *asset* critici
- Copertura della capacità di individuazione e di reazione di tutte le funzioni critiche
- Considerazione di cyber-minacce specifiche agli istituti in esercitazioni di ripristino

Banche cat. 4-5

Focus dell’attività di vigilanza

- Valutazione dei risultati ottenuti dalle società di audit esterne sul programma di audit standard «Gestione dei cyber-rischi»
- Monitoraggio dei piani di misure inoltrati

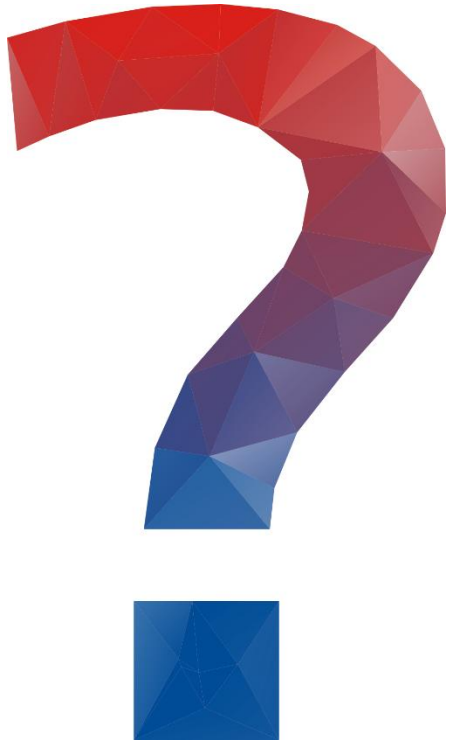
Strumenti di vigilanza impiegati

- Svolgimento di controlli in loco
- Sviluppo di un programma di audit standard «Gestione dei cyber-rischi»

Temi critici

- Considerazione dei requisiti di sicurezza per la copertura dei cyber-rischi presso i fornitori critici
- Maggiore sensibilizzazione della direzione/del consiglio direttivo per i cyber-rischi (integrazione dei cyber-rischi nella gestione operativa dei rischi)

finma



finma

GRAZIE PER L'ATTENZIONE!