Erkenntnisse aus Vor-Ort-Kontrollen

Kleinbankensymposium – 7. September 2026

Agenda

1

Übersicht zu den Vor-Ort-Kontrollen

- Risikobasierte Aufsicht
- Unterschied zwischen den Aufsichtsinstrumenten
- Proportionalitätsprinzip
- Statistiken
- Hohe und sehr hohe Risiken

2

Fokusthemen

- Geldwäscherei – und Terrorismusfinanzierung
- Hypotheken
- Cyber

3

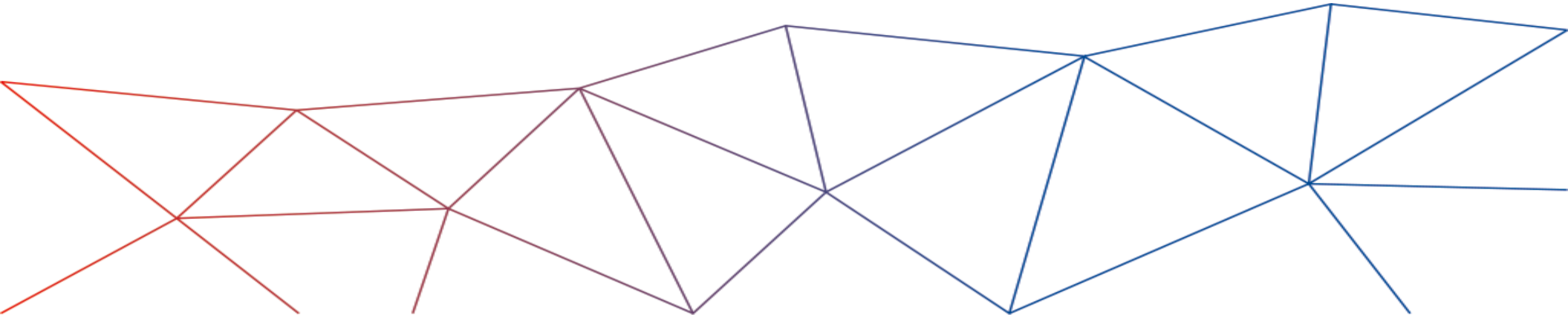
Abschluss

- Fragen

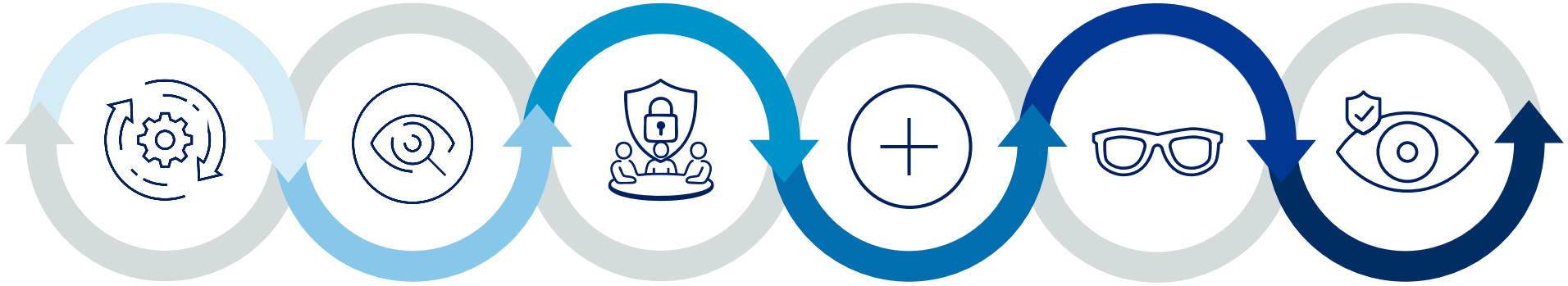
finma

Übersicht zu den Vor-Ort-Kontrollen

Banken und Wertpapierhäuser



Risikobasierte Aufsicht



Veränderung der Risikosituation

Risikoorientierter Einsatz der Aufsichtsinstrumente inkl. Vor-Ort-Kontrollen

Höhere Prüfdichte und vertiefte Prüfungen

Mehr identifizierte Feststellungen

Verbesserte Transparenz

Neue Einschätzung der Risikosituation

Risikobasierte Aufsicht führt bei erhöhtem Prüfungsumfang zu einer höheren Transparenz über bestehende Risiken.

Unterschiede zwischen den Aufsichtsinstrumenten

	Indirekte Aufsichtsinstrumente: u.a. Aufsichtsprüfung durch Prüfgesellschaften	Direkte Aufsichtsinstrumente: u.a. Vor-Ort-Kontrollen
Prüfrahmen	Prüfung definierter aufsichtsrechtlicher Prüfgebiete	Flexible und vertiefte Prüfung ausgewählter Aufsichts- und Risikothemen
Umfang & Tiefe	Die Intensität der Überwachung hängt, wie vom Gesetzgeber vorgesehen, von der Bewilligungsform und zugleich von der Risikobeurteilung der FINMA ab.	Flexible, risikoorientierte Festlegung der Prüftiefe
Vorgehen	Durch Prüfgesellschaft nach festgelegten Prüfstandards	Bedarfsgerechte Wahl geeigneter Aufsichts- bzw. Prüfhandlungen
Beurteilung	Unabhängiges Prüfurteil und Berichterstattung an FINMA	Eigene aufsichtsrechtliche Risikobeurteilung der FINMA
Ergebnis	**Prüfbericht mit Beanstandungen und Empfehlungen**	**Aufsichtsrechtliche Erkenntnisse und ggf. Massnahmen der FINMA**

Grundlagen

Finanzmarktaufsichtsgesetz (FINMAG) Art. 24ff., insb. Art 27 und 29 sowie Art 31 ff.
Finanzmarktprüfverordnung (FINMA-PV) und Aufsichtsprüfverordnung FINMA
FINMA-Rundschreiben 2025/1 Prüfwesen

Proportionalitätsprinzip

Anzahl Vor-Ort-Kontrollen	2023		2024		2025	
	Total	Ø pro Institut	Total	Ø pro Institut	Total	Ø pro Institut
Kat. 1	33	**33**	45	**45**	47	**47**
Kat. 2	10	**3,3**	15	**5,0**	14	**4,7**
Kat. 3	34	**1,2**	34	**1,3**	35	**1,3**
Kat. 4	10	**0,2**	6	**0,1**	11	**0,2**
Kat. 5	7	**0,05**	10	**0,06**	10	**0,06**
n/a*	0	**n/a**	1	**n/a**	1	**n/a**

** Vor-Ort-Kontrollen bei externen Dienstleistern*

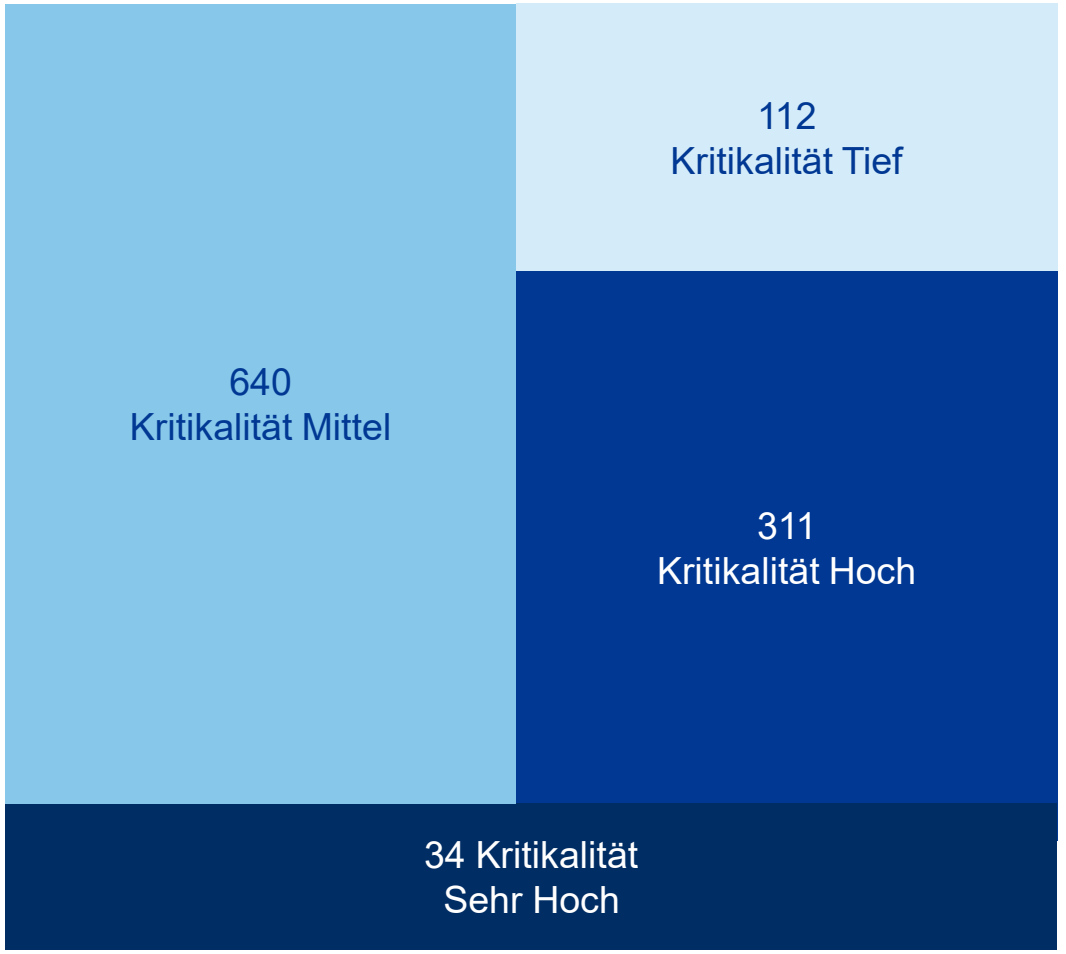
Statistiken

3 Jahre (2023-2025)

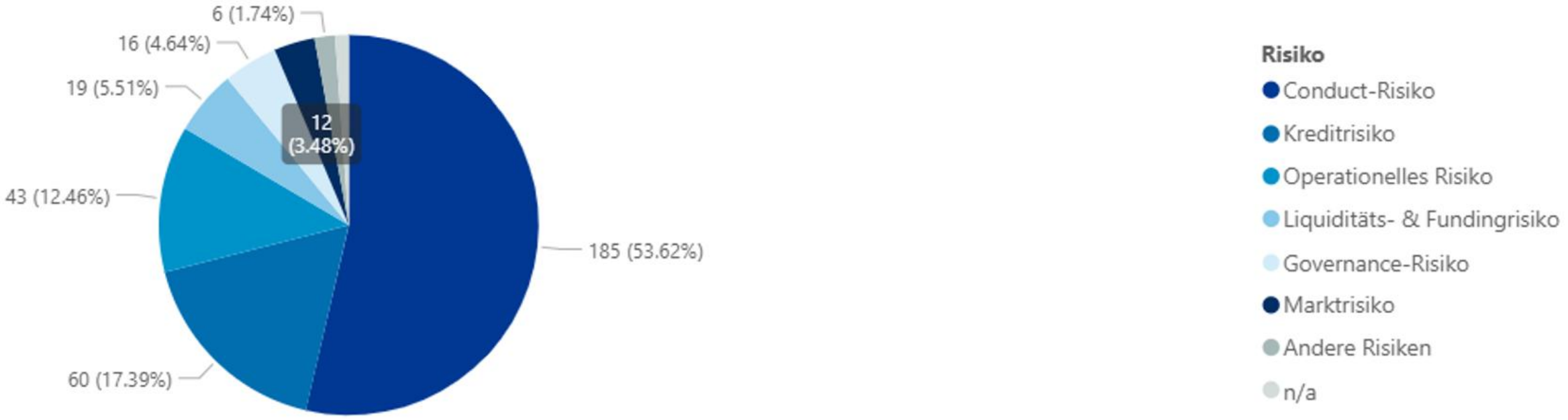
71 Institute (Kategorie 2-5)

198 Vor-Ort-Kontrollen

1097 Feststellungen

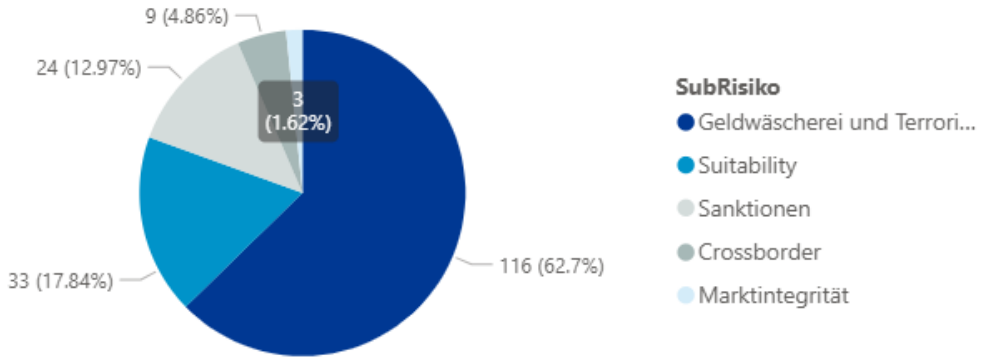


Feststellungen mit hohen und sehr hohen Risiken – Übersicht

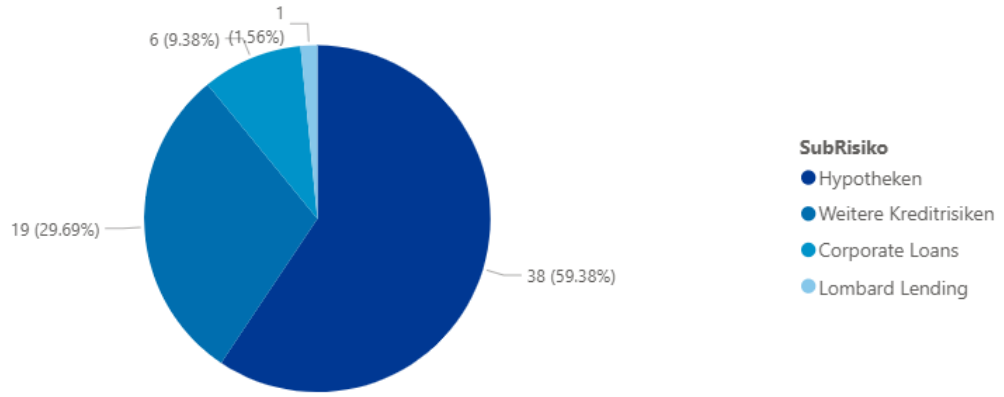


Feststellungen mit hohen und sehr hohen Risiken – Hauptthemen

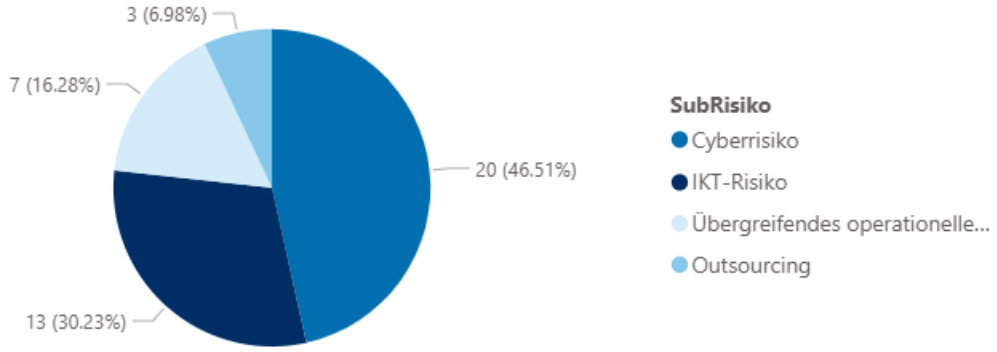
Conduct-Risiko



Kreditrisiko



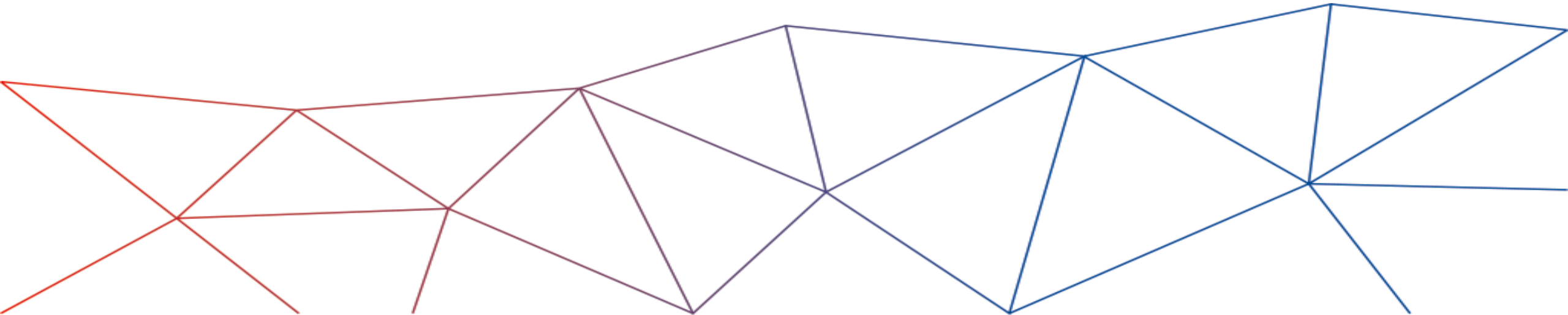
Operationelles Risiko



finma

Fokusthema

Geldwäscherei – und Terrorismusfinanzierung (GwG)



Allgemeine Prinzipien – Aufsichtserwartung der FINMA zum Thema 'GwG'

Risikotoleranz

Ein wirkungsvolles Geldwäscherei abwehrdispositiv setzt eine durch das Oberleitungsorgan des Finanzintermediärs klar definierte Risikotoleranz voraus (tone from the top). Gewisse besonders risikoreiche Kundensegmente und Dienstleistungen sind auszuschliessen.

Meldung und Zusammenarbeit

Verdächtige Sachverhalte werden unverzüglich der Meldestelle für Geldwäscherei (MROS) gemeldet. Die Institute arbeiten angemessen mit den Behörden zusammen.

Risikobasierter Ansatz

Die Institute wenden einen risikobasierten Ansatz an, um ihre GW/TF-Risiken zu identifizieren, zu beurteilen, zu steuern und zu überwachen. Massnahmen sind auf das Risikoprofil abgestimmt.

Schulung und Sensibiliserung

Die Mitarbeitenden sind regelmässig und angemessen zu schulen. Die Institute fördern eine Kultur der Integrität und Sensibilisierung für GW/TF-Risiken.

Kunden und Geschäftspartner

Die Institute führen angemessene Sorgfaltspflichten durch, kennen ihre Kunden und Geschäftspartner und verstehen den Zweck und die Art der Geschäftsbeziehung.

Kontrolle und Sicherheit

Angemessene interne Kontrollen, unabhängige Prüfungen und regelmässige Wirksamkeitsprüfungen stellen sicher, dass die Massnahmen wirksam und angemessen sind.

Transaktionsüberwachung

Die Institute überwachen Geschäftsbeziehungen und Transaktionen kontinuierlich, um ungewöhnliche oder verdächtige Aktivitäten zu erkennen und abzuklären.

Dokumentation

Die Institute dokumentieren ihre GW/TF-Risiken, Massnahmen, Entscheide und Kontrollen vollständig, nachvollziehbar und aktuell.

Grundlage | Diese Prinzipien basieren auf dem Geldwäschereigesetz (GwG), der Geldwäschereiverordnung (GwV-FINMA) sowie auf FINMA-Rundschreiben.

Feststellungen der FINMA zum Thema 'GwG'

Anzahl VOK[1]

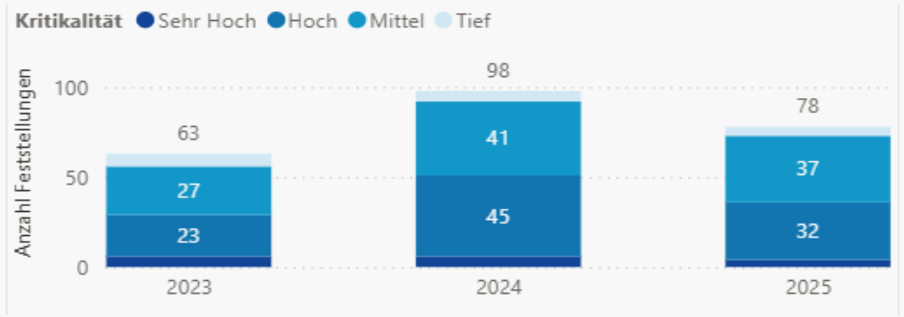
im Zeitraum

33

Ø Anzahl Feststellungen

pro VOK

7.24



KYC-Dokumentation

- Wiederkehrende Schwächen im Zusammenhang mit *cross-booking* Geschäftsbeziehungen.
- Verspätungen bei der periodischen Überprüfung von Geschäftsbeziehungen.

Erkennung von TmeR

- Erkennung lediglich von sog. "AML hits", welche nicht auf der Definition von TmeR gemäss Art. 14 GwV-FINMA basieren.
- Durchlauftransaktionen nur im Fall von Barein- oder Barauszahlungen berücksichtigt; nicht in bar ausgeführte Durchlauftransaktionen nicht systemunterstützt erkannt.

Risikotoleranz

- Hohe Risikotoleranz bezüglich Kunden mit hohen Reputationsrisiken (z.B. Kunden, die in öffentlichkeitswirksame Rechtsstreitigkeiten verwickelt sind, in heiklen Industrien tätig sind oder eine Nähe zu Potentaten aufweisen).

1 Anzahl VOK mit Feststellungen zum Fokusthema

Zentrale Risiken im GwG-Bereich

Vermögensverwaltung

Insbesondere im Vermögensverwaltungsbereich können nach wie vor hohe Risiken beobachtet wer den, die durch das Abwehrdispositiv nicht in adäquater Weise überwacht und begrenzt werden. Politisch exponierte Personen (z. B. Amtsträger oder Verantwortliche in staatlichen oder staatsnahen Unternehmen) aus Hochrisikoländern bergen als Kundschaft besonders hohe Geld wäscherei- sowie Rechts- und Reputationsrisiken für Finanzintermediäre.

Retailbanking

Mängel bei der Kombination von statischen und dynamischen Kriterien bzw. Szenarien im Transaktionsmonitoring führen dazu, dass einerseits verdächtige Transaktionen nicht erkannt werden, andererseits zu einer Vielzahl von falsch-positiven Alerts. Insbesondere bei Bartransaktionen besteht die Gefahr, dass die Szenarien zu deren Überwachung im Transaktionsmonitoring fehlen oder ungeeignet sind, um auffällige Bartransaktionen oder Durchlauftransaktionen zu erkennen.

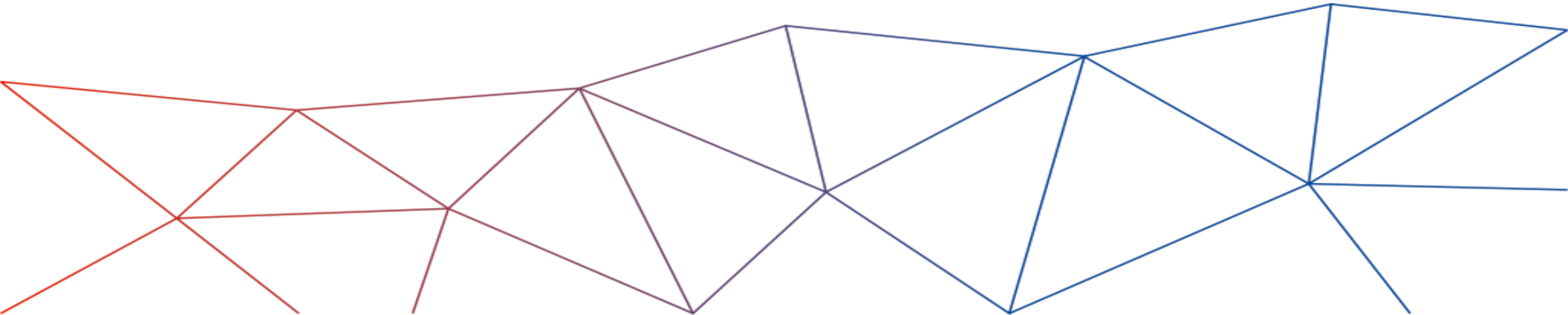
Krypto

Im Kryptobereich sind die Geldwäschereirisiken hoch. Kryptowährungen werden häufig als Zahlungsmittel bei Cyberattacken, bei illegalem Onlinehandel oder zur Umgehung von Sanktionen verwendet.

finma

Fokusthema

Hypotheken



finma

Allgemeine Prinzipien – Aufsichtserwartung der FINMA zum Thema 'Hypotheken'

Solide Kreditvergabe

Hypotheken werden nur an solvente Kunden vergeben. Die Tragbarkeit wird sorgfältig geprüft und angemessen dokumentiert.

Dokumentation

Kreditentscheide, Tragbarkeitsberechnungen, Belehnungen und Sicherheiten sind vollständig, nachvollziehbar und aktuell zu dokumentieren.

Angemessene Belehnung

Die Belehnung entspricht den regulatorischen Vorgaben. Eigenmittel und allfällige Zusatzsicherheiten werden angemessen berücksichtigt.

Prozesse und Kompetenzen

Klare Prozesse, Zuständigkeiten und Kontrollen stellen eine einheitliche Anwendung sicher. Mitarbeitende verfügen über die erforderlichen Kompetenzen.

Risikobasierte Beurteilung und Pricing

Die Beurteilung der Kreditrisiken ist risikobasiert. Dies fliesst in das Pricing sowie in Kreditentscheide und Auflagen ein.

Umgang mit Markt- und Objektwertrisiken

Markt- und Objektwertrisiken werden angemessen berücksichtigt. Bewertungen sind konservativ, plausibel und regelmässig zu überprüfen.

Überwachung und Früherkennung

Die Institute überwachen Hypothekarportfolios kontinuierlich und erkennen Risiken frühzeitig. Bei Bedarf werden geeignete Massnahmen ergriffen.

Vermeidung von Interessenkonflikten

Interessenkonflikte werden identifiziert, vermieden und – wo unvermeidbar – transparent gemacht und angemessen gemanagt.

Grundlage

Diese Prinzipien basieren auf dem Bankengesetz (BankG), der Bankenverordnung (BankV) sowie auf FINMA-Rundschreiben und -Aufsichtsmitteilungen (insbesondere Aufsichtsmitteilung 02/2025).

Feststellungen der FINMA zum Thema 'Hypotheken'

Anzahl VOK [1]

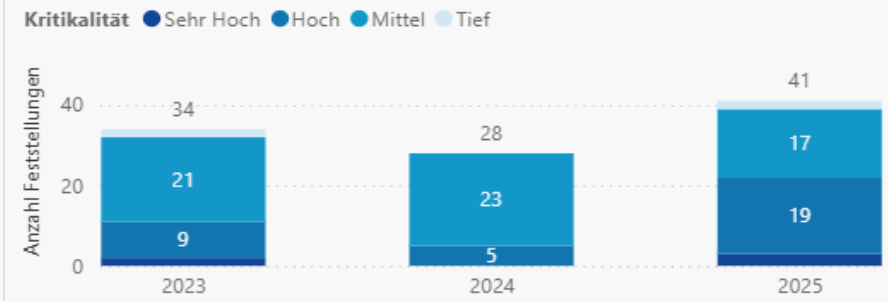
im Zeitraum

18

Ø Anzahl Feststellungen

pro VOK

5.72



Organisation der Kontrollfunktionen und IKS

- Fehlende unabhängige Kontrolle der durch die Front-Office-Einheiten getroffenen Kreditentscheide
- Fehlende unabhängige Kontrollen der vorgenommenen Immobilienbewertungen (durch Front oder Immobilienschätzer)

Immobilienbewertung und diesbezügliche Kontrollen

- Fehlende Qualifikations- und Erfahrungsanforderungen für Mitarbeitende aus dem Front Office, die Immobilienbewertungen vornehmen
- Ungenügende Sicherstellung der Unabhängigkeit von Immobilienbewertungen

Beurteilung der Tragbarkeit

- Nicht nachhaltige Tragbarkeitskriterien
- Ungenügendes EtP-Reporting und fehlende Datengrundlage für konsistentes Monitoring der EtP-Entwicklung über mehrere Quartale

1 Anzahl VOK mit Feststellungen zum Fokusthema

Unterschiede je nach Aufsichtskategorie zum Thema 'Hypotheken'

Der aufsichtsrechtliche Fokus im Bereich Hypotheken und die eingesetzten Aufsichtsinstrumente sind über die Aufsichtskategorien hinweg grundsätzlich gleich. Die Unterschiede liegen primär in der Intensität, Tiefe und Häufigkeit der risikoorientierten Aufsicht unter Berücksichtigung von **Grösse**, **Geschäftsmodell** und **Risikoprofil** des Instituts.

Fokus der Aufsichtstätigkeit

- Risikomanagement & Governance
- Kreditvergabe & Kreditrichtlinien
- Kreditüberwachung & Internes Kontrollsystem
- Bewertung & Sicherheiten
- Recovery & Wertberichtigungen
- Eigenmittelverordnung

Eingesetzte Aufsichtsinstrumente

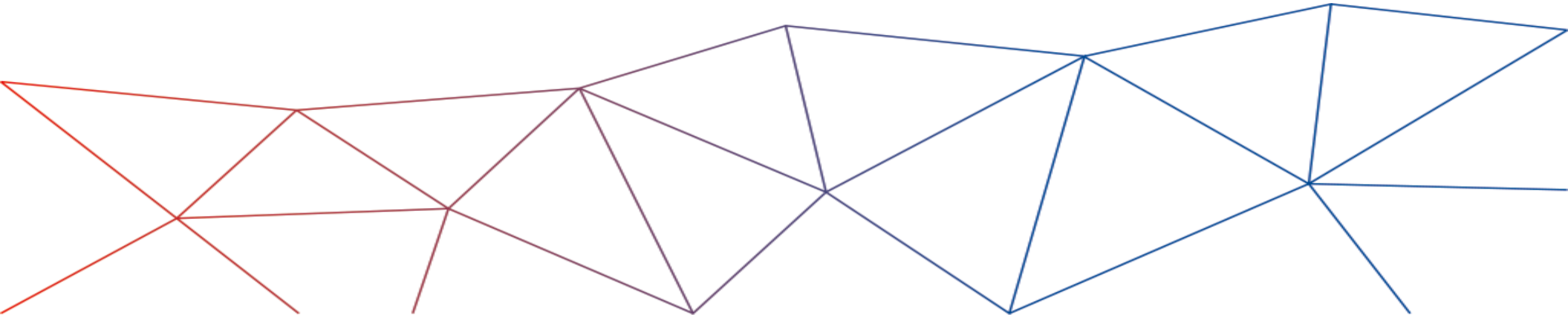
- Vor-Ort-Kontrollen / Deep Dives
- Aufsichtsgespräche
- Reporting / Datenanalysen / EHP-Umfragen
- Analysen der Prüfberichte
- Stresstests & Analysen

Kritische Themen

- Hohe EtP-Quoten
- Tragbarkeitskriterien
- Immobilienmarkt und Zinsentwicklung

Fokusthema

Cyber



Allgemeine Prinzipien – Aufsichtserwartung der FINMA zum Thema 'Cyber'

Governance und Verantwortung

Der Verwaltungsrat und die Geschäftsleitung tragen die Gesamtverantwortung für die Cyber-Resilienz, Rollen, Verantwortlichkeiten und Kompetenzen sind klar definiert und angemessen organisiert.

Erkennung und Reaktion

Cyber-Vorfälle werden frühzeitig erkannt, strukturiert behandelt und gemeldet. Die Institute verfügen über wirksame Reaktions- und Eskalationsprozesse und arbeiten mit den Behörden zusammen.

Risikomanagement

Die Institute identifizieren, beurteilen und steuern Cyber-Risiken systematisch. Massnahmen sind risikobasiert und in die Gesamtrisikosteuerung integriert.

Drittparteien und Lieferketten

Cyber-Risiken aus Auslagerungen und Drittparteien werden angemessen gesteuert. Verträge, Überwachung und Exit-Strategien stellen die fortlaufende Kontrolle sicher.

Technische und organisatorische Sicherheit

Die Institute implementieren angemessene technische und organisatorische Massnahmen, um Vertraulichkeit, Integrität, Verfügbarkeit und Authentizität zu gewährleisten.

Tests und Resilienz

Regelmässige Tests (z.B. Vulnerability Scans, Penetration Tests, Tabletop-Übungen) überprüfen die Wirksamkeit der Massnahmen und stärken die Resilienz.

Daten und Identitäten

Der Schutz von Daten und Identitäten ist gewährleistet. Zugriff erfolgt nach dem Prinzip der minimalen Rechte (Least Privilege), Datensicherung und Wiederherstellung sind sichergestellt.

Überwachung und kontinuierliche Verbesserung

Cyber-Risiken und Kontrollmassnahmen werden fortlaufend überwacht und verbessert. Erkenntnisse aus Vorfällen und Änderungen werden systematisch berücksichtigt.

Grundlage

Diese Prinzipien basieren auf den FINMA-Rundschreiben 'Operationelle Risiken – Banken' (2023/1) sowie den Aufsichtserwartungen der FINMA.

Feststellungen der FINMA zum Thema 'Cyber'

Anzahl VOK [1]

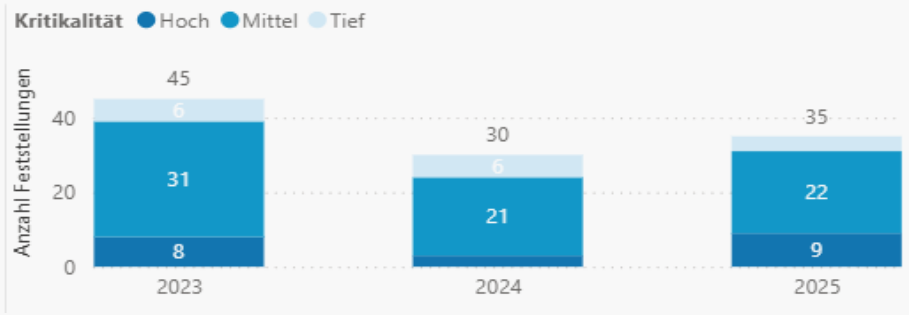
im Zeitraum

16

Ø Anzahl Feststellungen

pro VOK

6.88



Risikosteuerung

- Keine eigenständige Definition von Cyber-Risiken
- Hohe Risikotoleranz für kritischer Datendiebstahl, Datenverlust oder Verletzung des Datenschutzes

Verwundbarkeitsanalysen und Penetrationstests

- Fehlende Verwundbarkeitsanalysen des internen Netzwerks
- Fehlende Strategie sowie unzureichende Vorgaben für die Durchführung von Penetrationstests
- Unzureichende Einhaltung der gemäss FINMA-RS 2023/1 geforderten Regelmässigkeit bei der Durchführung von Verwundbarkeitsanalysen und Penetrationstests

Reaktionsfähigkeiten

- Unzureichende zeitnahe Reaktionsfähigkeit
- Ungenügende Entwicklung und Implementierung von Prozessen zur Reaktion auf Cyber-Schwachstellen

1 Anzahl VOK mit Feststellungen zum Fokusthema

Unterschiede je nach Aufsichtskategorie zum Thema 'Cyber'

Banken Kat. 2-3

Fokus der Aufsichtstätigkeit

- Szenariobasierte Cyber-Übungen (sog. Red-Teaming bei Kat. 2)
- Einbettung von Cyber-Risiken in das operationelle Risikomanagement
- Operationalisierung und Einbindung einer Cyber-Threat-Landscape in das Reporting an das Management

Eingesetzte Aufsichtsinstrumente

- Durchführung von Vor-Ort-Kontrollen
- Thematisierung von Cyber-Risiken in Aufsichtsgesprächen
- Cyber-Meldewesen und Berücksichtigung von Third Party Provider

Kritische Themen

- Unzureichende Inventarisierung kritischer Assets
- Abdeckung der Erkennungs- und Reaktionsfähigkeit aller kritischen Funktionen
- Berücksichtigung institutsspezifischer Cyber-Bedrohungen in Wiederherstellungsübungen

Banken Kat. 4-5

Fokus der Aufsichtstätigkeit

- Auswertung der Ergebnisse der externen Prüfgesellschaften zum Standardprüfprogramm „Management von Cyberrisiken”
- Nachverfolgung der eingereichten Massnahmenpläne

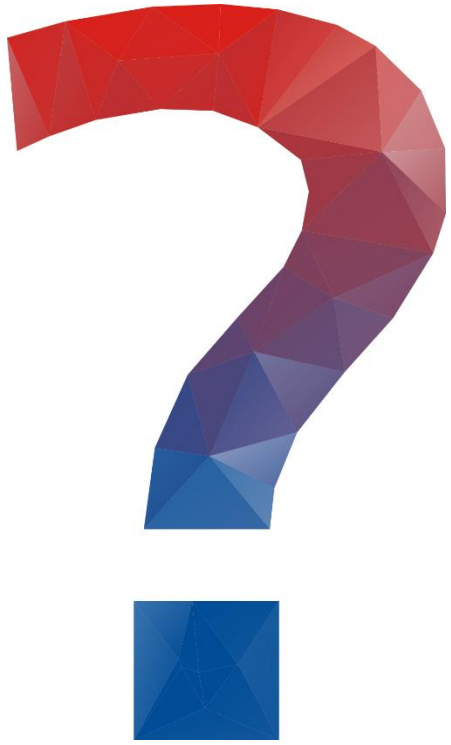
Eingesetzte Aufsichtsinstrumente

- Durchführung von Vor-Ort-Kontrollen
- Entwicklung eines Standardprüfprogramms zum "Management von Cyber-Risiken"

Kritische Themen

- Berücksichtigung von Sicherheitsanforderungen zur Abdeckung von Cyber-Risiken bei kritischen Dienstleistern
- Erhöhung der Sensibilität der Geschäftsleitung/des Vorstands für Cyber-Risiken (Einbindung von Cyber-Risiken in das operationelle Risikomanagement)

finma



finma

HERZLICHEN DANK!