Enseignements tirés des contrôles sur place

Symposium des petites Banques – 7 septembre 2026

Programme

1

Vue d’ensemble des contrôles sur place

- Surveillance basée sur les risques
- Différence entre les instruments de surveillance
- Principe de proportionnalité
- Statistiques
- Risques élevés et très élevés

2

Thèmes prioritaires

- Blanchiment d’argent et financement du terrorisme
- Hypothèques
- Cybersécurité

3

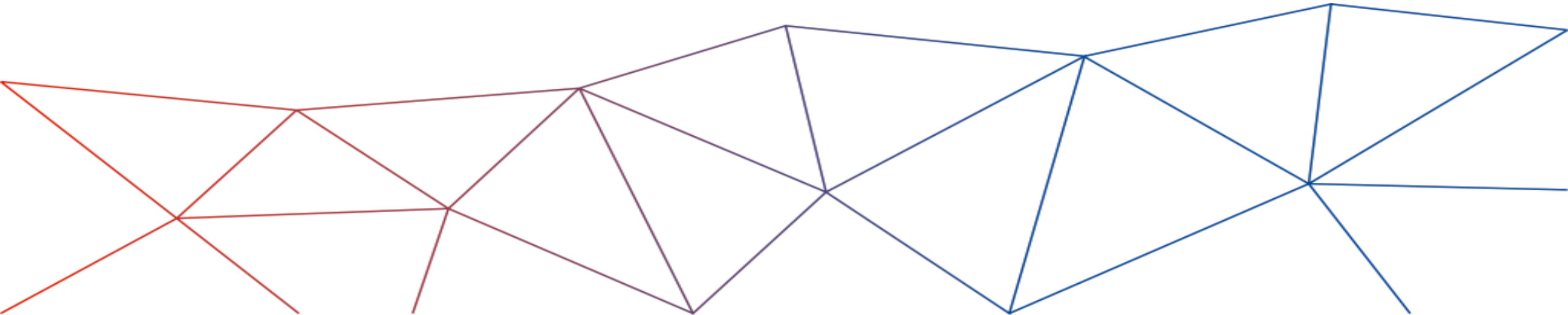
Conclusion

- Questions

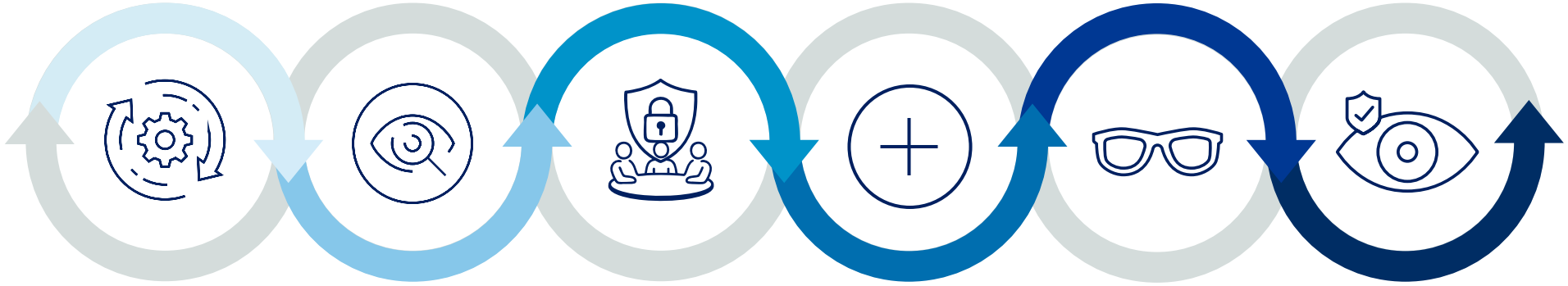
finma

Vue d’ensemble des contrôles sur place

Banques et maisons de titres



Surveillance basée sur les risques



Évolution de la situation en matière de risques

Utilisation des instruments de surveillance axée sur les risques, y c. contrôles sur place

Intensification et approfondissement des contrôles

Augmentation du nombre de constatations

Transparence accrue

Réévaluation de la situation en matière de risques

En élargissant le champ de l'audit, la surveillance axée sur les risques offre une transparence accrue sur les risques existants.

Différences entre les instruments de surveillance

	Instruments de surveillance indirects: notamment audit prudentiel par des sociétés d'audit	Instruments de surveillance directs: notamment contrôles sur place
Cadre des audits	Examen de domaines d'audit prudentiel définis	Examen flexible et approfondi de sujets ciblés ayant trait à la surveillance et au risque
Étendue et intensité de contrôle	Niveau de contrôle standardisé et axé sur les risques, conformément aux directives de la FINMA	Définition flexible et axée sur les risques de l'étendue et de l'intensité de contrôle
Procédure	Par la société d'audit selon des normes d'audit établies	Choix des activités de surveillance et d'audit en fonction des besoins
Évaluation	Attestation d'audit indépendante et établissement de rapports à l'intention de la FINMA	Propre évaluation prudentielle des risques par la FINMA
Résultat	**Rapport d'audit portant sur les contestations et les recommandations**	**Constats prudentiels et, le cas échéant, mesures de la FINMA**

Bases

Loi sur la surveillance des marchés financiers (LFINMA) art. 24ss, en particulier les art. 27 et 29 ainsi que les art. 31ss
Ordonnance sur les audits des marchés financiers (OA-FINMA) et ordonnance de la FINMA sur l'audit prudentiel
Circulaire FINMA 2025/1 Activités d'audit

Principe de proportionnalité

Nombre de contrôles sur place	2023		2024		2025	
	Total	Ø par établissement	Total	Ø par établissement	Total	Ø par établissement
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**
s/o*	0	**n/a**	1	**n/a**	1	**s/o**

** Contrôles sur place auprès de prestataires externes*

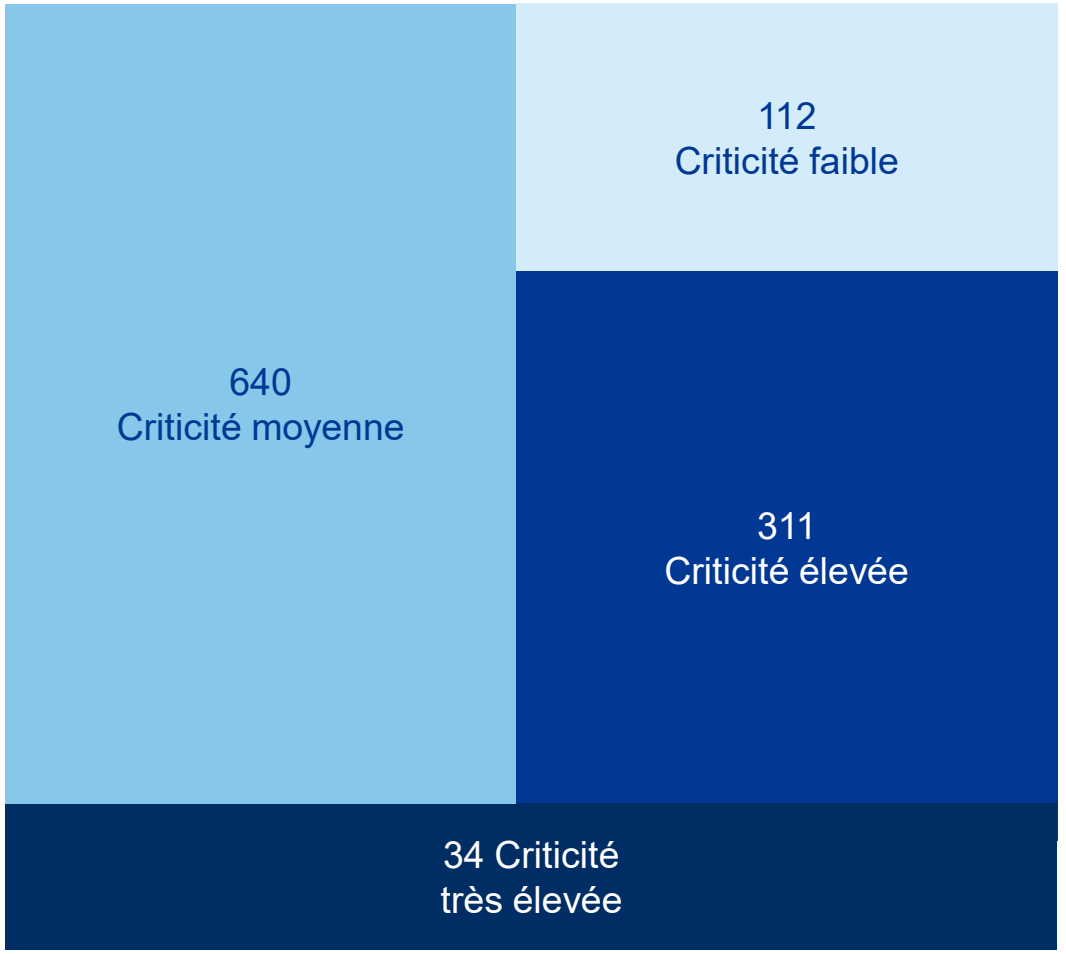
Statistiques

3 ans (2023 à 2025)

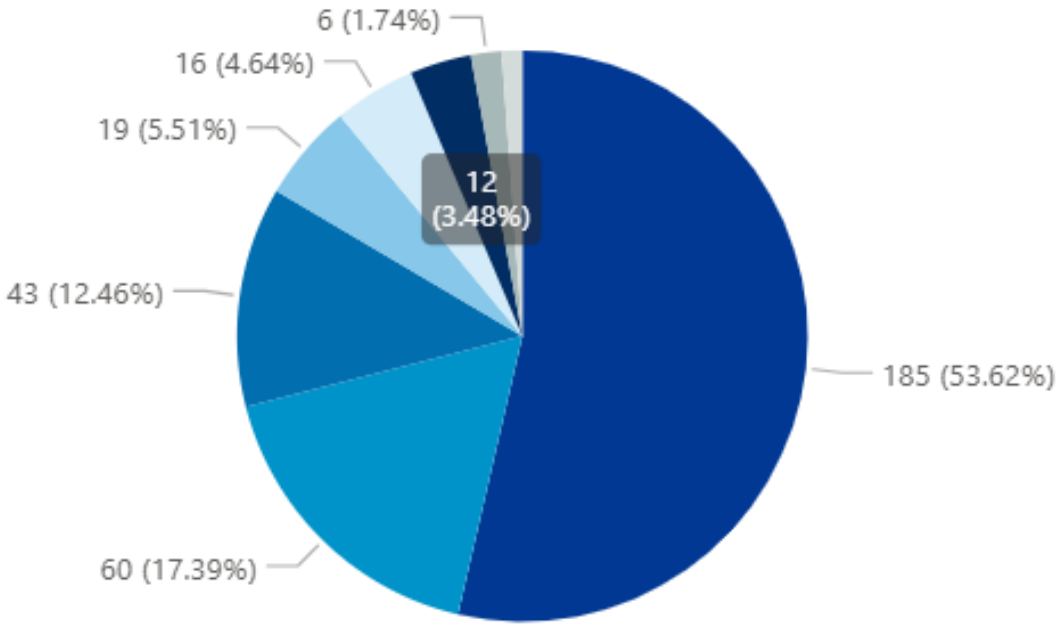
71 établissements (catégories 2 à 5)

198 contrôles sur place

1097 constatations

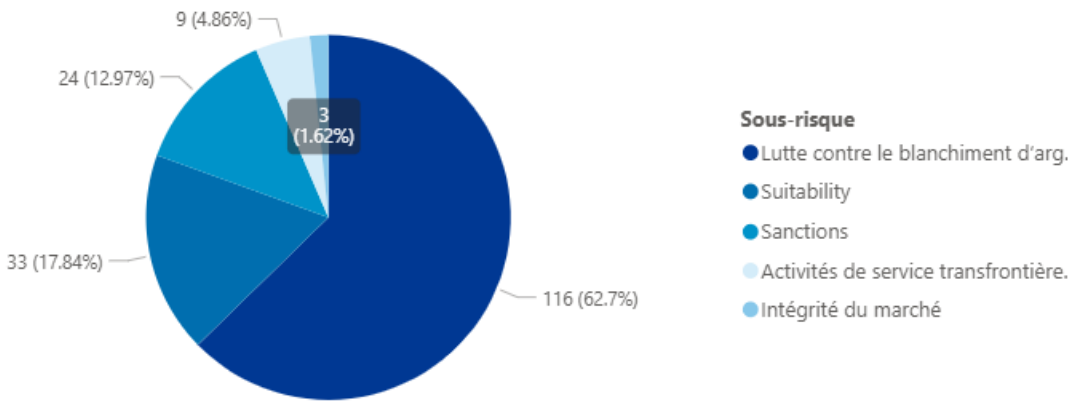


Constatations présentant des risques élevés et très élevés – vue d'ensemble

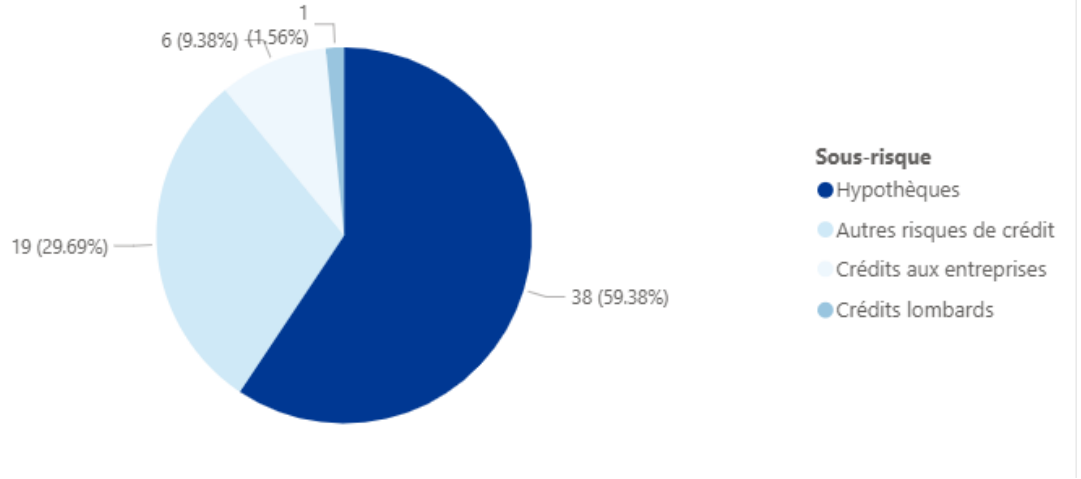


Constatations présentant des risques élevés et très élevés – thèmes principaux

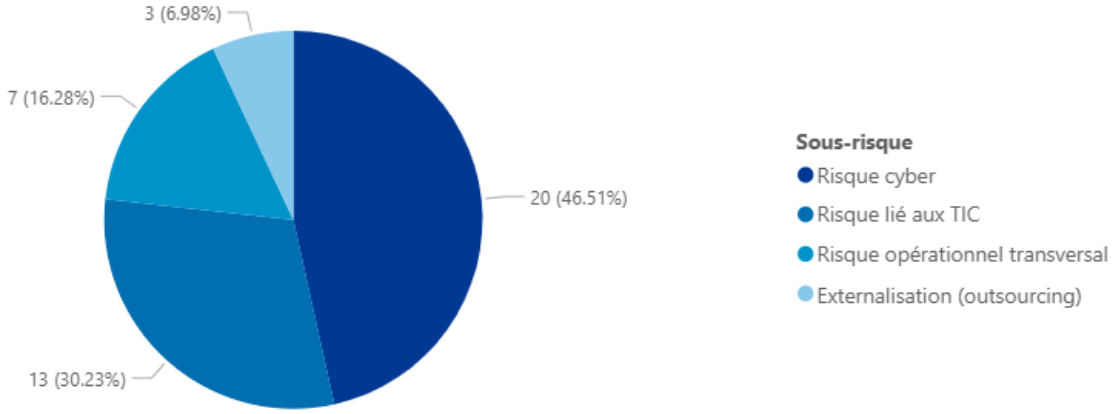
Conduite (*conduct*)



Risque de crédit

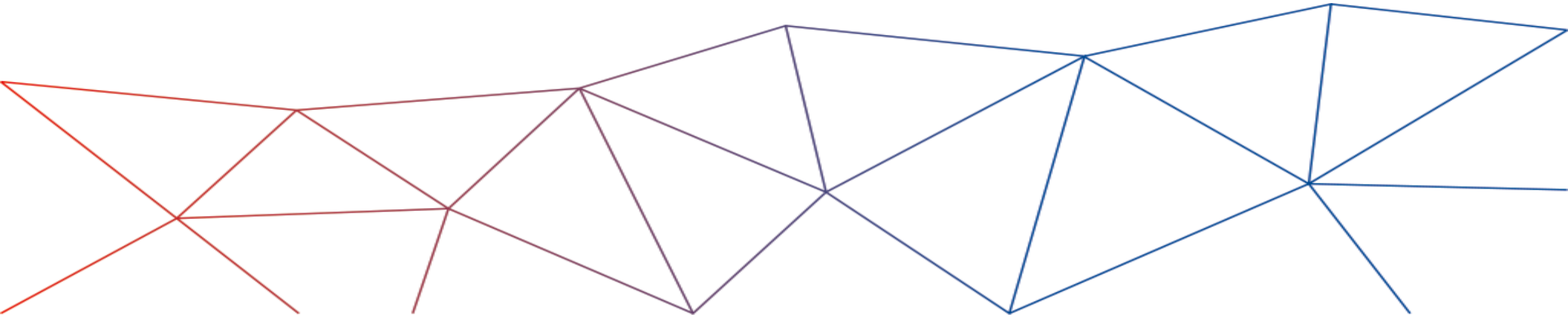


Risque opérationnel



Thème prioritaire

Blanchiment d’argent et financement du terrorisme (LBA)



Principes généraux – attentes de la FINMA en matière de surveillance concernant la LBA

Tolérance au risque

Un dispositif efficace de lutte contre le blanchiment d'argent présuppose une tolérance au risque clairement définie par l'organe responsable de la haute direction de l'intermédiaire financier (*tone from the top*). Certains segments de clientèle et prestations particulièrement risqués doivent être exclus.

Approche fondée sur les risques

Les établissements appliquent une approche fondée sur les risques pour identifier, évaluer, gérer et surveiller leurs risques de BA/FT. Les mesures sont adaptées au profil de risque.

Clients et partenaires commerciaux

Les établissements exercent leurs devoirs de diligence de manière adéquate, connaissent leurs clients et partenaires commerciaux, et comprennent le but et la nature de la relation d'affaires.

Surveillance des transactions

Les établissements surveillent en permanence les relations d'affaires et les transactions afin de détecter et d'examiner toute activité inhabituelle ou suspecte.

Communication et collaboration

Les faits suspects sont immédiatement communiqués au Bureau de communication en matière de blanchiment d'argent (MROS). Les établissements collaborent de manière adéquate avec les autorités.

Formation et sensibilisation

Les collaborateurs sont formés régulièrement et de manière adéquate. Les établissements favorisent une culture de l'intégrité et la sensibilisation aux risques en matière de BA/FT.

Contrôle et sécurité

Des contrôles internes adéquats, des audits indépendants et des contrôles réguliers de l'efficacité garantissent que les mesures sont efficaces et adaptées.

Documentation

Les établissements tiennent une documentation complète, traçable et actualisée de leurs risques en matière de BA/FT, des mesures prises, des décisions adoptées et des contrôles effectués.

Base

Ces principes reposent sur la loi sur le blanchiment d'argent (LBA), l'ordonnance de la FINMA sur le blanchiment d'argent (OBA-FINMA) ainsi que sur les circulaires de la FINMA.

Constatations de la FINMA concernant la LBA

Nombre de contrôles sur place[1]

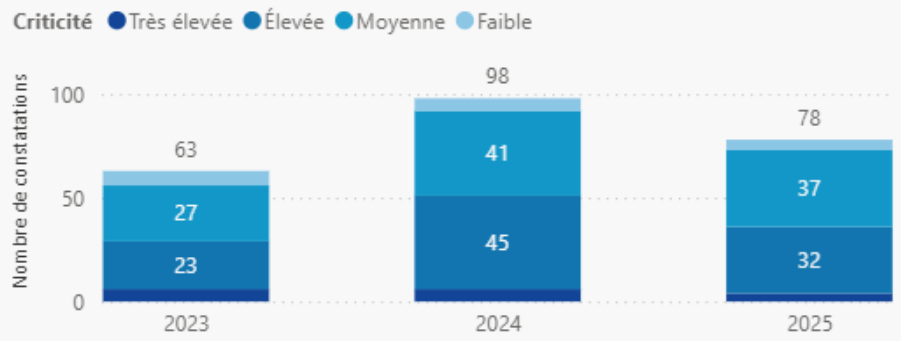
durant la période sous revue

33

Nombre moyen de constatations

par contrôle sur place

7.24



Documentation KYC

- Lacunes récurrentes en lien avec les relations d'affaires *cross-booking*.
- Retards dans la vérification périodique des relations d'affaires.

Détection des TRA

- Détection limitée aux seules alertes AML, qui ne reposent pas sur la définition des transactions comportant des risques accrus (TRA) au sens de l'art. 14 OBA-FINMA.
- Opérations de passage uniquement prises en compte en cas de versements ou retraits d'espèces; les opérations non effectuées en numéraire ne sont pas détectées par le système informatique.

Tolérance au risque

- Tolérance au risque élevée à l'égard de clients présentant des risques de réputation élevés (p. ex. clients impliqués dans des litiges très médiatisés, actifs dans des secteurs sensibles ou entretenant des liens avec des potentats).

[1] Nombre de CSP ayant donné lieu à des constatations concernant le thème prioritaire

Principaux risques dans le champ d’application de la LBA

Gestion de fortune

Des risques élevés continuent d’être observés, en particulier dans le domaine de la gestion de fortune, sans qu’ils ne soient surveillés et limités de manière adéquate par le dispositif de contrôle interne. En tant que clients, les personnes politiquement exposées (p. ex. personnages publics ou dirigeants d’entreprises publiques ou semi-publiques) issues de pays à haut risque présentent pour les intermédiaires financiers des risques de blanchiment d’argent, ainsi que des risques juridiques et de réputation particulièrement élevés.

Banque de détail

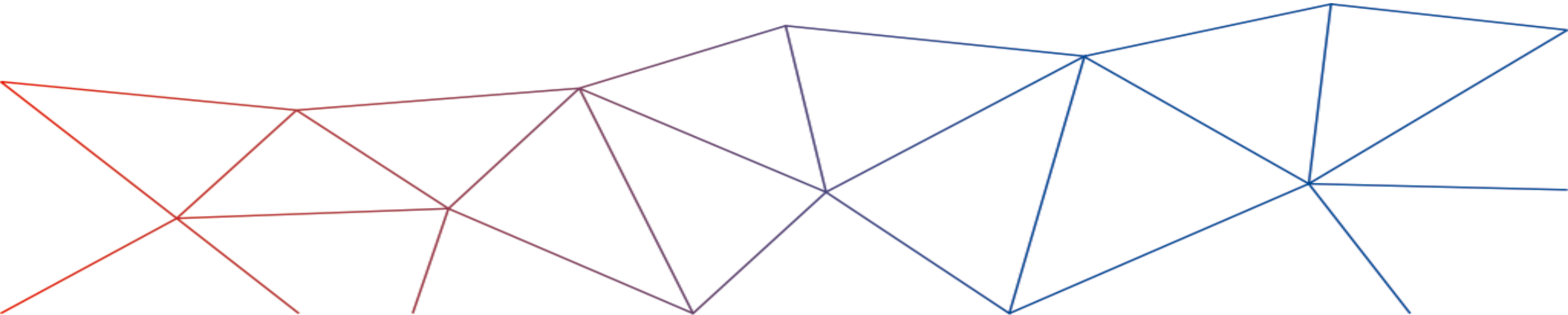
Mängel bei der Kombination von statischen und dynamischen Kriterien bzw. Szenarien im Transaktionsmonitoring führen dazu, dass einerseits verdächtige Transaktionen nicht erkannt werden, andererseits zu einer Vielzahl von falsch-positiven Alerts. Insbesondere bei Bartransaktionen besteht die Gefahr, dass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

Cryptomonnaies

Les risques de blanchiment d’argent sont élevés dans le secteur des cryptomonnaies. Ces dernières sont fréquemment utilisées comme moyen de paiement lors de cyberattaques, dans le cadre du commerce illégal en ligne ou pour le contournement de sanctions.

Thème prioritaire

Hypothèques



Principes généraux – attentes de la FINMA en matière de surveillance concernant les hypothèques

Octroi prudent de crédits

Les hypothèques ne sont accordées qu'à des clients solvables. La capacité financière est examinée minutieusement et documentée de manière adéquate.

Documentation

Les décisions d'octroi de crédit, calculs de capacité financière, taux de nantissement et garanties doivent faire l'objet d'une documentation exhaustive, traçable et actualisée.

Taux de nantissement adéquat

Le taux de nantissement est conforme aux exigences réglementaires. Les fonds propres et les éventuelles garanties supplémentaires sont pris en compte de manière adéquate.

Processus et compétences

Des processus, responsabilités et contrôles clairs garantissent une application uniforme. Les collaborateurs disposent des compétences requises.

Évaluation et tarification fondées sur les risques

L'évaluation des risques de crédit est fondée sur les risques. Elle est intégrée dans la tarification, ainsi que dans les décisions d'octroi de crédit et les conditions afférentes.

Gestion des risques de marché et des risques liés à la valeur des biens

Les risques de marché et les risques liés à la valeur des biens sont pris en compte de manière adéquate. Les évaluations doivent être prudentes, plausibles et révisées régulièrement.

Surveillance et détection précoce

Les établissements surveillent en permanence les portefeuilles hypothécaires et détectent les risques en temps utile. Des mesures appropriées sont prises, le cas échéant.

Prévention des conflits d'intérêts

Les conflits d'intérêts sont identifiés, évités et, lorsqu'ils sont inévitables, divulgués en toute transparence et gérés de manière adéquate.

Base

Ces principes reposent sur la loi sur les banques (LB), l'ordonnance sur les banques (OB) ainsi que sur les circulaires et communications FINMA sur la surveillance (en particulier la communication sur la surveillance 02/2025).

Constatations de la FINMA concernant les hypothèques

Nombre de contrôles sur place[1]

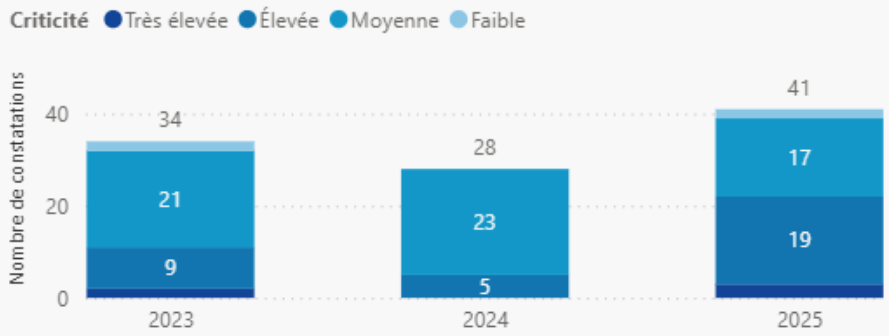
durant la période sous revue

18

Nombre moyen de constatations

par contrôle sur place

5.72



Organisation des fonctions de contrôle et SCI

- Absence de contrôle indépendant des décisions d'octroi de crédit prises par les unités de *front office*
- Absence de contrôles indépendants des évaluations immobilières réalisées (par le *front office* ou par des experts en estimations immobilières)

Évaluation immobilière et contrôles afférents

- Absence d'exigences de qualification et d'expérience pour les collaborateurs du *front office* réalisant des évaluations immobilières
- Garantie insuffisante de l'indépendance des évaluations immobilières

Évaluation de la capacité financière

- Critères de capacité financière non durables
- Rapports EtP insuffisants et manque de données de base pour un suivi cohérent de l'évolution des EtP sur plusieurs trimestres

1 Nombre de CSP ayant donné lieu à des constatations concernant le thème prioritaire

Différences selon la catégorie de surveillance concernant les hypothèques

L'approche prudentielle dans le domaine hypothécaire et les instruments de surveillance utilisés sont en principe identiques d'une catégorie de surveillance à l'autre. Les différences résident principalement dans l'intensité, la profondeur et la fréquence de la surveillance axée sur les risques, compte tenu de la **taille**, du **modèle d'affaires** et du **profil de risque** de l'établissement.

Priorité de l'activité de surveillance

- Gestion des risques et gouvernance
- Octroi de crédits et directives en matière d'octroi de crédit
- Surveillance des crédits et système de contrôle interne
- Évaluation et garanties
- *Recovery* et corrections de valeur
- Ordonnance sur les fonds propres

Instruments de surveillance utilisés

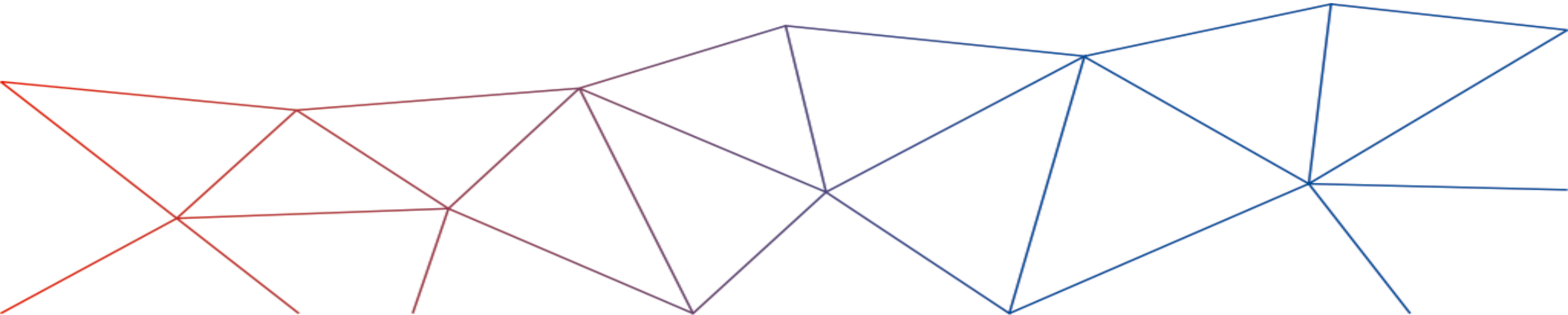
- Contrôles sur place / *deep dives*
- Entretiens de surveillance
- Rapports / analyses de données / enquêtes EHP
- Analyses des rapports d'audit
- Tests de résistance et analyses

Sujets critiques

- Ratios élevés d'EtP
- Critères de capacité financière
- Marché immobilier et évolution des taux d'intérêt

Thème prioritaire

Cybersécurité



Principes généraux – attentes de la FINMA en matière de surveillance concernant la cybersécurité

Gouvernance et responsabilité

Le conseil d'administration et la direction assument la responsabilité générale de la cyberrésilience; les rôles, responsabilités et compétences sont clairement définis et organisés de manière adéquate.

Détection et réaction

Les cyberincidents sont détectés à un stade précoce, traités de manière structurée et signalés. Les établissements disposent de processus de réaction et d'escalade efficaces, et collaborent avec les autorités.

Gestion des risques

Les établissements identifient, évaluent et gèrent les cyberrisques de manière systématique. Les mesures sont fondées sur les risques et intégrées dans la gestion globale des risques.

Tiers et chaînes d'approvisionnement

Les cyberrisques découlant d'externalisations et de tiers sont pilotés de manière adéquate. Les contrats, la surveillance et les stratégies de sortie garantissent un contrôle continu.

Sécurité technique et organisationnelle

Les établissements mettent en œuvre des mesures techniques et organisationnelles adéquates pour garantir la confidentialité, l'intégrité, la disponibilité et l'authenticité.

Tests et résilience

Des tests réguliers (p. ex. analyses de vulnérabilité, tests d'intrusion, exercices sur table) vérifient l'efficacité des mesures et renforcent la résilience.

Données et identités

La protection des données et des identités est garantie. Les accès sont octroyés selon le principe du moindre privilège (*least privilege*); la sauvegarde et la restauration des données sont assurées.

Surveillance et amélioration continue

Les cyberrisques et les mesures de contrôle font l'objet d'une surveillance et d'une amélioration continues. Les enseignements tirés des incidents et des changements sont pris en compte de manière systématique.

Base

Ces principes reposent sur la circulaire FINMA 2023/1 «Risques opérationnels – banques» ainsi que sur les attentes de la FINMA en matière de surveillance.

Constatations de la FINMA concernant la cybersécurité

Nombre de contrôles sur place[1]

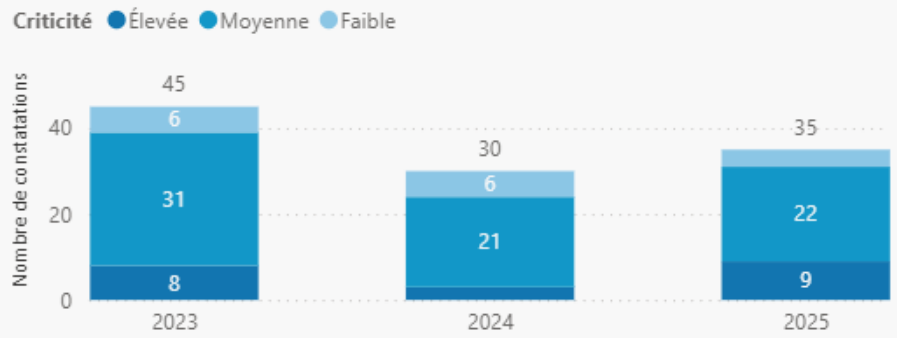
durant la période sous revue

16

Nombre moyen de constatations

par contrôle sur place

6.88



Gestion des risques

- Absence de définition autonome des cyberrisques
- Tolérance au risque élevée en matière de vol de données critiques, de perte de données ou d'atteinte à la protection des données

Analyses de vulnérabilité et tests d'intrusion

- Absence d'analyses de vulnérabilité du réseau interne
- Absence de stratégie et directives insuffisantes pour la réalisation de tests d'intrusion
- Respect insuffisant de la périodicité requise par la circulaire FINMA 2023/1 pour la réalisation d'analyses de vulnérabilité et de tests d'intrusion

Capacités de réaction

- Capacité de réaction rapide insuffisante
- Développement et mise en œuvre insuffisants des processus de réaction aux vulnérabilités

1 Nombre de CSP ayant donné lieu à des constatations concernant le thème prioritaire

Différences selon la catégorie de surveillance concernant la cybersécurité

Banques cat. 2 à 3

Priorité de l'activité de surveillance

- Exercices de cybersécurité basés sur des scénarios (*red teaming* pour la cat. 2)
- Intégration des cyberrisques dans la gestion des risques opérationnels
- Opérationnalisation et intégration d'une cartographie des cybermenaces dans les rapports destinés à la direction

Instruments de surveillance utilisés

- Réalisation de contrôles sur place
- Traitement des cyberrisques lors des entretiens de surveillance
- Système d'annonce des cyberincidents et prise en compte des prestataires tiers

Sujets critiques

- Inventaire insuffisant des actifs critiques
- Couverture de la capacité de détection et de réaction pour l'ensemble des fonctions critiques
- Prise en compte des cybermenaces propres à l'établissement dans les tests de restauration

Banques cat. 4 à 5

Priorité de l'activité de surveillance

- Évaluation des résultats des sociétés d'audit externes relatifs au programme d'audit standard «Gestion des cyberrisques»
- Suivi des plans de mesures soumis

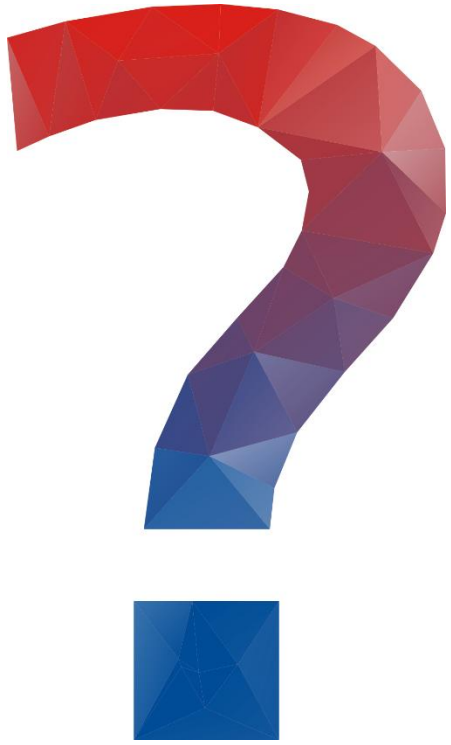
Instruments de surveillance utilisés

- Réalisation de contrôles sur place
- Élaboration d'un programme d'audit standard sur la «Gestion des cyberrisques»

Sujets critiques

- Prise en compte des exigences en matière de sécurité couvrant les cyberrisques chez les prestataires critiques
- Sensibilisation accrue de la direction / du comité aux cyberrisques (intégration des cyberrisques dans la gestion des risques opérationnels)

finma



finma

MERCI!