Findings from on-site inspections

Small Bank Symposium – 7 September 2026

Agenda

1

Overview of on-site inspections

- Risk-based supervision
- Difference between the supervisory instruments
- Principle of proportionality
- Statistics
- High and very high risks

2

Focus areas

- Money laundering – and terrorist financing
- Mortgages
- Cyber

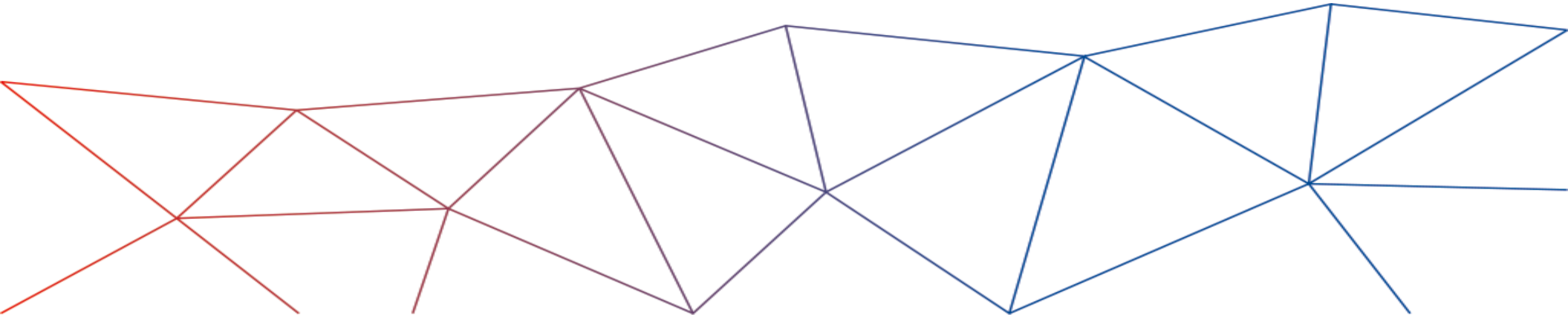
3

Conclusion

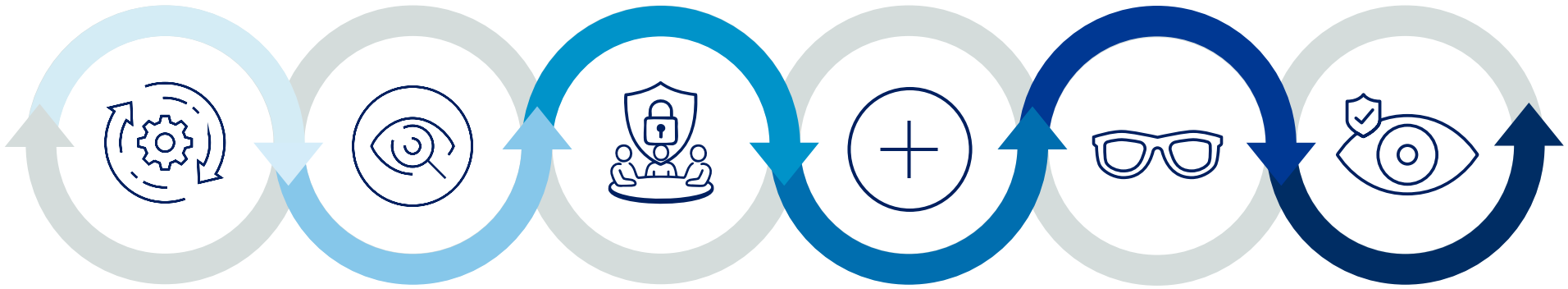
- Questions

Overview of on-site inspections

Banks and securities firms



Risk-based supervision



Changes to the risk situation

Risk-based usage of supervisory instruments, incl. on-site inspections

Increased inspection frequency and in-depth inspections

More findings identified

Improved transparency

New assessment of the risk situation

Risk-based supervision with increased inspection scope leads to improved transparency of existing risks.

Difference between the supervisory instruments

	Indirect supervisory instruments: including supervisory inspections carried out by audit firms	Direct supervisory instruments: including on-site inspections
Inspection framework	Inspection of defined regulatory audit areas	Flexible and in-depth inspection of selected supervisory and risk areas
Scope & depth	Standardised, risk-focused depth of inspection, in accordance with FINMA guidelines	Flexible, risk-focused approach to setting the level of scrutiny
Procedure	Carried out by an audit firm in accordance with established auditing standards	Needs-based choice of appropriate supervisory and/or audit procedures
Evaluation	Independent audit opinion and reporting to FINMA	Own regulatory risk assessment by FINMA
Result	**Audit report containing issues and recommendations**	**Supervisory findings by FINMA with measures where required**

Basic principles

Financial Market Supervision Act (FINMASA) Art. 24 ff., esp. Arts. 27 and 29 as well as Art 31 ff.
Financial Market Auditing Ordinance (FINMA-PV) and FINMA Regulatory Auditing Ordinance
FINMA Circular 2025/1 "Auditing"

Principle of proportionality

Quantity On-site inspections	2023		2024		2025	
	Total	Ø per institution	Total	Ø per institution	Total	Ø per institution
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**

** On-site inspections of external service providers*

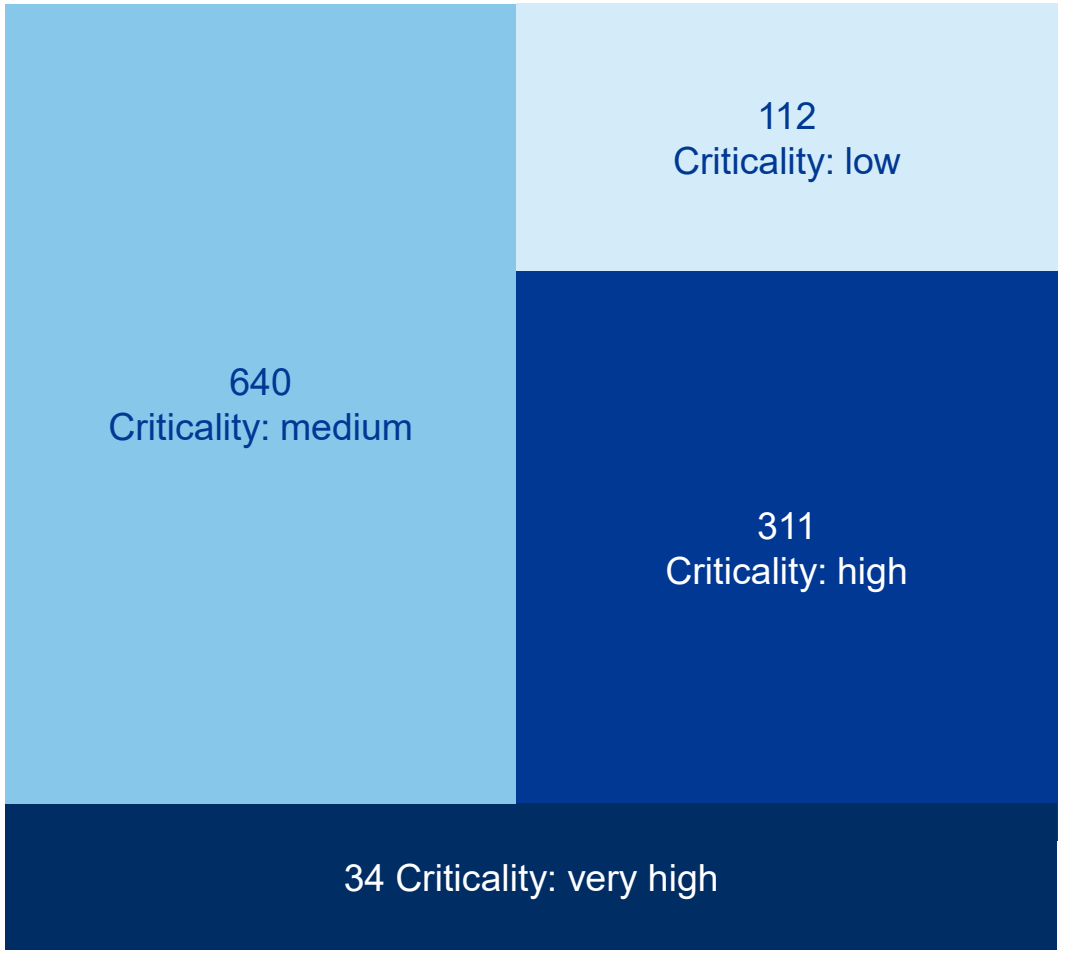
Statistics

3 years (2023-2025)

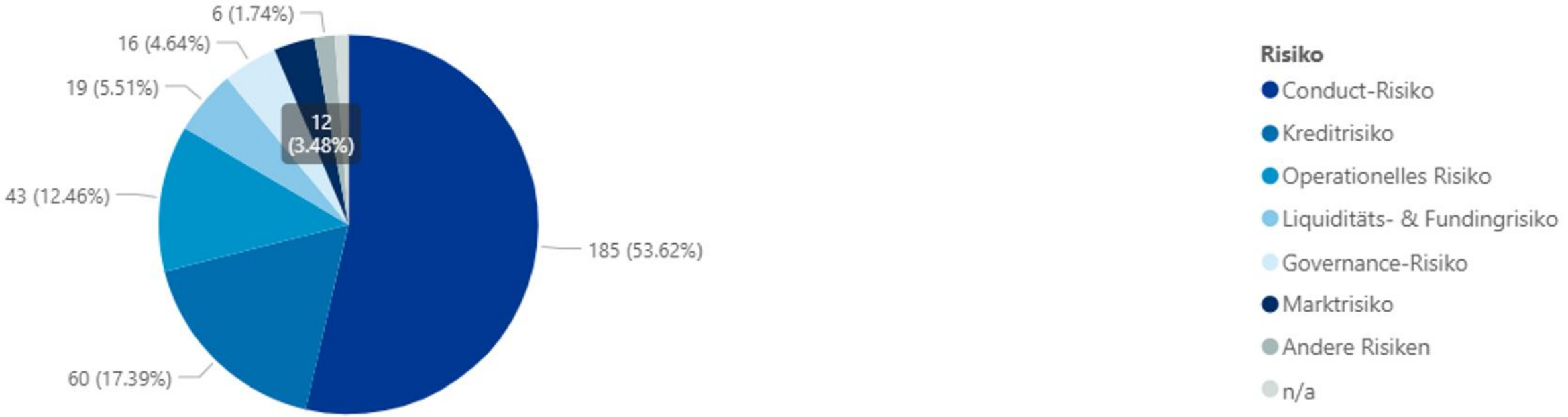
71 institutions (category 2-5)

198 on-site inspections

1097 findings

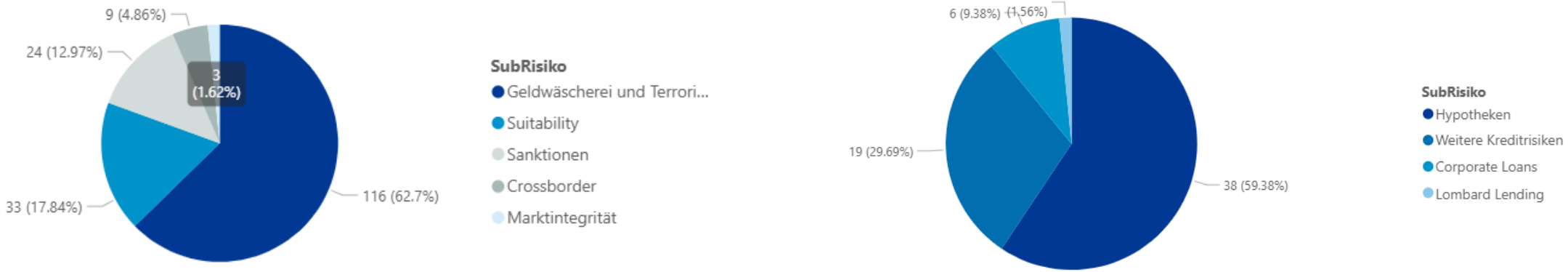


Findings with high and very high risk levels – overview



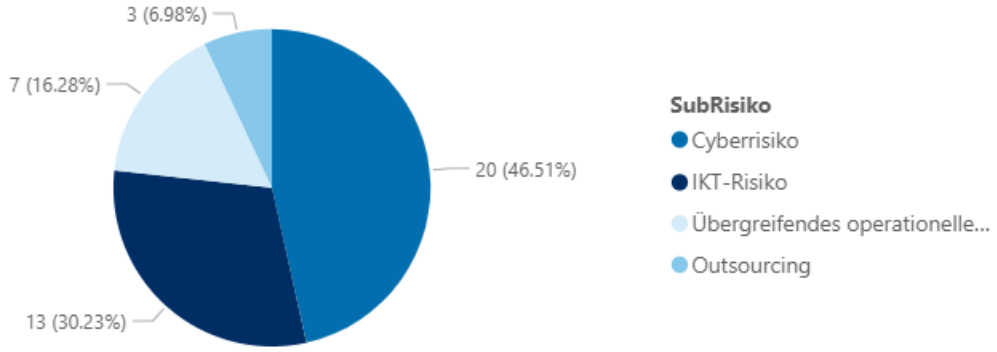
Findings with high and very high risk levels – key themes

Conduct risk



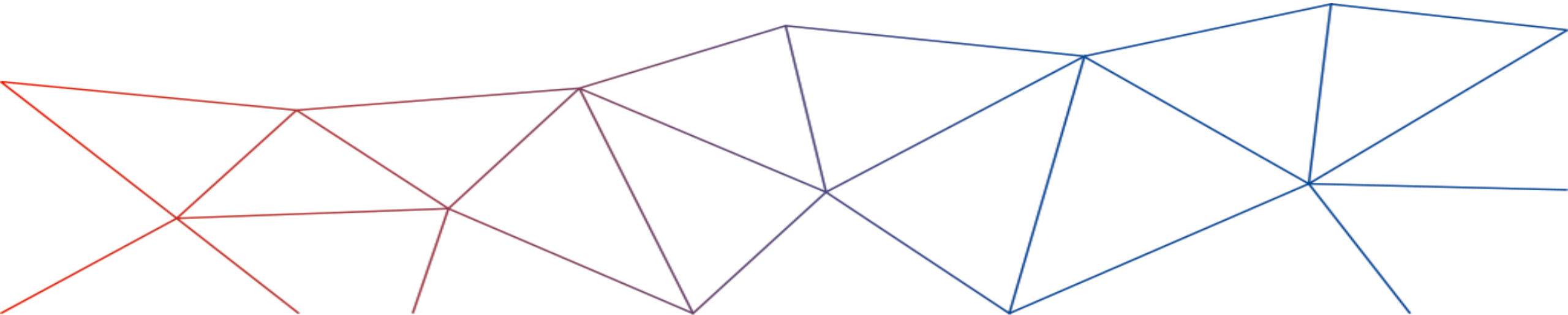
Credit risk

Operational risk



Key theme

Money laundering – and terrorist financing (AMLA)



General principles – FINMA's supervisory expectations relating to AMLA

Risk tolerance

An effective money laundering defence mechanism needs a risk tolerance which has been clearly defined by the financial intermediary's uppermost governing body (tone from the top). Certain customer segments and services, which are particularly risky, are to be excluded.

Risk-oriented approach

The institutions adopt a risk-based approach in order to identify, assess, manage and monitor their money laundering and terrorist financing risks. Measures are adapted to the risk profile.

Customers and business partners

The institutions carry out appropriate due diligence obligations, know their customers and business partners, and understand the purpose and nature of the business relationship.

Transaction monitoring

The institutions continually monitor business relationships and transactions in order to spot and clarify unusual or suspicious activity.

Reporting and cooperation

Suspicious circumstances are reported immediately to the Money Laundering Reporting Office Switzerland (MROS). The institutions cooperate appropriately with the authorities.

Training and awareness

Employees must be trained appropriately and regularly. The institutions promote a culture of integrity and awareness of money laundering and terrorist financing risks.

Monitoring and security

Appropriate internal controls, independent audits and regular effectiveness reviews ensure that the measures are effective and appropriate.

Documentation

The institutions document their money laundering and terrorist financing risks, measures, decisions and audits in a comprehensive, transparent and up-to-date manner.

Basis

These principles are based on the Anti-Money Laundering Act (AMLA), the Anti-Money Laundering Ordinance (AMLO-FINMA) and on the FINMA Circular.

FINMA's findings on the topic of AMLA

Anzahl VOK[1]

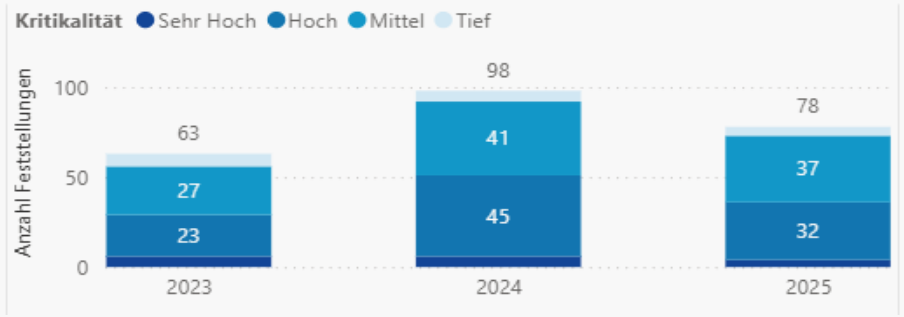
im Zeitraum

33

Ø Anzahl Feststellungen

pro VOK

7.24



KYC documentation

- Recurring weakness in connection with cross-booking business relationships.
- Delays in the periodic review of business relationships.

Recognising high-risk transactions

- Detection of what are known as "AML hits", which do not fall within the definition of a high-risk transaction in accordance with Art. 14 of the AMLO-FINMA.
- Pass-through transactions only taken into account in the case of cash receipts or cash withdrawals; pass-through transactions not carried out in cash not recognised by the system.

Risk tolerance

- High risk tolerance relating to customers with high reputational risk (e.g. customers who are involved in high-profile legal disputes, operate in sensitive industries or who are close to potentates).

[1] Number of on-site inspections with findings relating to the key theme

Central risks relating to the Anti-Money Laundering Act (AMLA)

Wealth management

In wealth management in particular, high risks continue to be seen which are not being monitored and restricted by the defence mechanism in a suitable manner. As customers, politically exposed persons (e.g. public officials or leaders in state-owned or state-affiliated enterprises) from high-risk countries carry particularly high money laundering, legal and reputational risks for financial intermediaries.

Retail banking

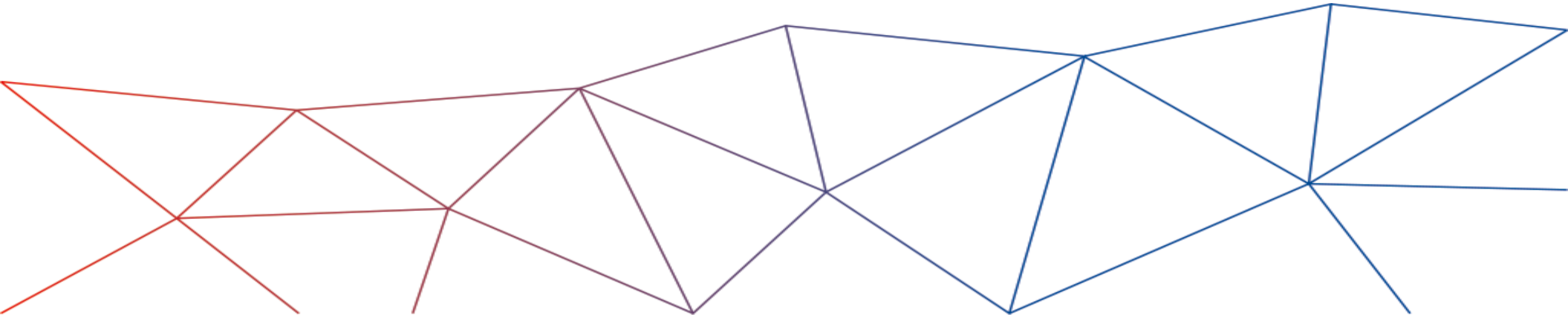
Shortcomings in the combination of static and dynamic criteria or scenarios in the transaction monitoring system lead to suspicious transactions not being identified and a wide range of false positive alerts at the same time. Especially for cash transactions, there is a risk that the scenarios for monitoring them in the transaction monitoring system are insufficient or unsuitable for identifying unusual cash transactions or pass-through transactions.

Crypto

There is a high risk of money laundering in crypto. Crypto currencies are often used as a payment method in cyberattacks, illegal online trading or to circumvent sanctions.

Key theme

Mortgages



General principles – FINMA's supervisory expectations relating to mortgages

Sound lending practices

Mortgages shall only be awarded to customers who are solvent. Affordability is checked and documented appropriately.

Documentation

Lending decisions, affordability calculations, mortgaging and security are to be documented fully and in a manner which is clear and up-to-date.

Appropriate loan-to-value limits

The loan-to-value limits conform with the regulatory requirements. Capital and any additional collateral is accounted for appropriately.

Processes and skills

Clear processes, responsibilities and controls are used to ensure consistency. Employees have the required skills.

Risk-based assessment and pricing

Assessment of the lending risk is risk-based. This is reflected in the pricing as well as the lending decisions and conditions.

Managing market and property value risks

Market and property value risks are accounted for appropriately. Valuations must be conservative, plausible and checked regularly.

Monitoring and early detection

Institutions monitor mortgage portfolios constantly and identify risks early. Appropriate measure are taken if required.

Avoiding conflicts of interest

Conflicts of interest are identified, avoided and – where unavoidable – made transparent and managed appropriately.

Basis

These principles are based on the Banking Act (BA), the Banking Ordinance (BO) and on the FINMA Circular, and FINMA Guidance (especially FINMA Guidance 02/2025).

FINMA's findings on the topic of mortgages

Anzahl VOK [1]

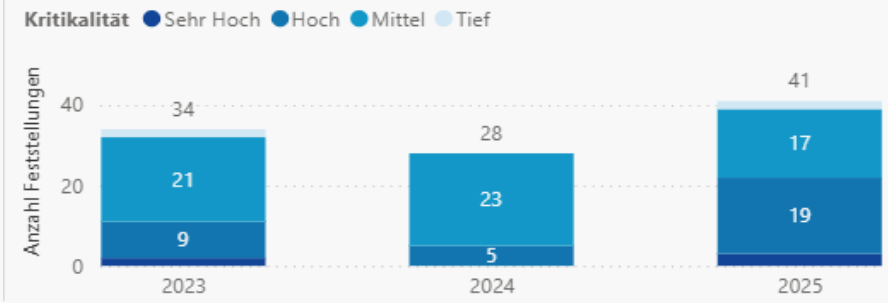
im Zeitraum

18

Ø Anzahl Feststellungen

pro VOK

5.72



Organisation of the control functions and ICS (internal control system)

- No independent controls on lending decisions made by front office units
- No independent controls on property valuations (by the front office or property valuers)

Valuation of property and the relevant controls

- No qualification and experience requirements for employees from the front office who carry out property valuations
- Inadequate safeguards to ensure the independence of property valuations

Affordability assessment

- Unsustainable affordability criteria
- Insufficient ETP reporting (loans which fall outside the banks' own lending criteria) and lack of data basis for consistent monitoring of the development of ETP loans over several quarters.

[1] Number of on-site inspections with findings relating to the key theme

Differences by supervisory category relating to mortgages

The supervisory focus on mortgages and the supervisory instruments used are essentially the same across the supervisory categories. The differences lie primarily in the intensity, depth and frequency of the risk-focused supervision, considering the institution's **size**, **business model** and **risk profile.**

Focus of the supervision

- Risk management & governance
- Lending practices & policies
- Monitoring of lending & internal control system
- Valuation & collateral
- Recovery & value adjustments
- Capital Adequacy Ordinance

Supervisory instruments used

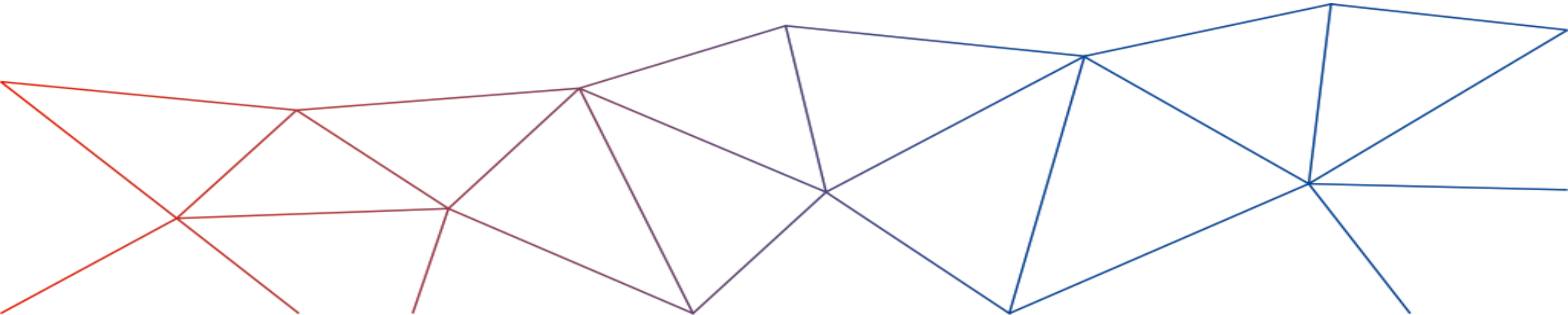
- On-site inspections / deep dives
- Supervisory meetings
- Reporting / data analyses / EHP surveys
- Audit report analyses
- Stress tests & analyses

Critical issues

- High ETP rates
- Affordability criteria
- Property market and interest rate development

Key theme

Cyber



General principles – FINMA's supervisory expectations relating to cyber

Governance and accountability

The Board of Directors and the Executive Board bear full responsibility for cyber resilience. Roles, responsibilities, and skills are clearly defined and organised appropriately.

Risk management

The institutions identify, assess and manage cyber risks systematically. Measures are risk-based and integrated into the overall risk management programme.

Technical and organisational security

The institutions implement appropriate technical and organisational measures to guarantee confidentiality, integrity, availability and authenticity.

Data and identities

Protection of data and identities is guaranteed. Access is granted according to the principle of least privilege; data security and recovery are ensured.

Identification and response

Cyber incidents are identified early, dealt with in a structured manner and reported. The institutions have effective response and escalation processes in place, and cooperate with the authorities.

Third parties and delivery chains

Cyber risks arising from outsourcing and third parties are managed appropriately. Contracts, monitoring and exit strategies ensure ongoing control.

Tests and resilience

Regular tests (e.g. vulnerability scans, penetration tests, tabletop exercises) check the effectiveness of the measures and strengthen resilience.

Monitoring and continuous improvement

Cyber risks and control measures are monitored and improved on an ongoing basis. Lessons learnt from incidents and changes are systematically included in considerations.

Basis

These principles are based on the FINMA Circular 'Operational risks and resilience – banks' (2023/1) and FINMA's supervisory expectations.

FINMA's findings on the topic of cyber

1

Anzahl VOK

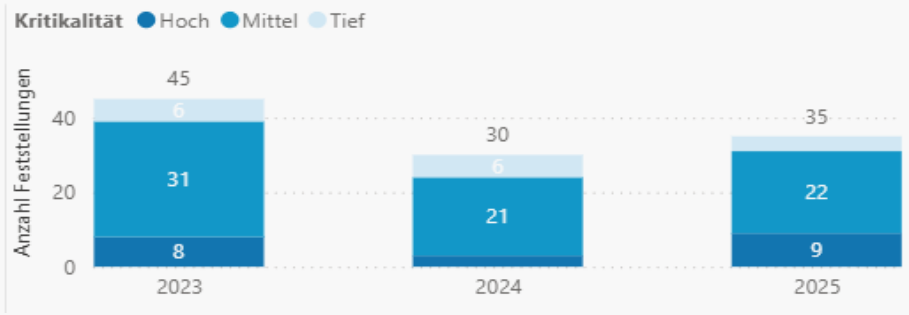
im Zeitraum

16

Ø Anzahl Feststellungen

pro VOK

6.88



Risk management

- No separate definition of cyber risks
- High risk tolerance for serious data theft, data loss or breach of data protection

Vulnerability analyses and penetration tests

- No vulnerability analysis for the internal network
- No strategy and inadequate guidelines for carrying out penetration tests
- Inadequate compliance with the regularity of vulnerability analyses and penetration tests as required under FINMA Circ. 2023/1

Ability to respond

- Inadequate ability to respond promptly
- Insufficient development and implementation of processes in response to cyber weaknesses

1 Number of on-site inspections with findings relating to the key theme

Differences by supervisory category relating to cyber

Banks cat. 2–3

Focus of the supervision

- Scenario-based cyber exercises (known as Red Teaming in cat. 2)
- Integrating cyber risks into operational risk management
- Operationalisation and integration of a cyber threat landscape into management reporting

Supervisory instruments used

- Carrying out on-site inspections
- Addressing the topic of cyber risks in supervisory meetings
- Cyber incident reporting and taking account of third-party providers

Critical issues

- Inadequate inventory of critical assets
- Addressing the detection and response capabilities of all critical functions
- Considering institution-specific cyber threats in recovery exercises

Banks cat. 4–5

Focus of the supervision

- Analysis of the results produced by the external audit firms for the standard audit programme "Cyber risk management”
- Following up on submitted plans

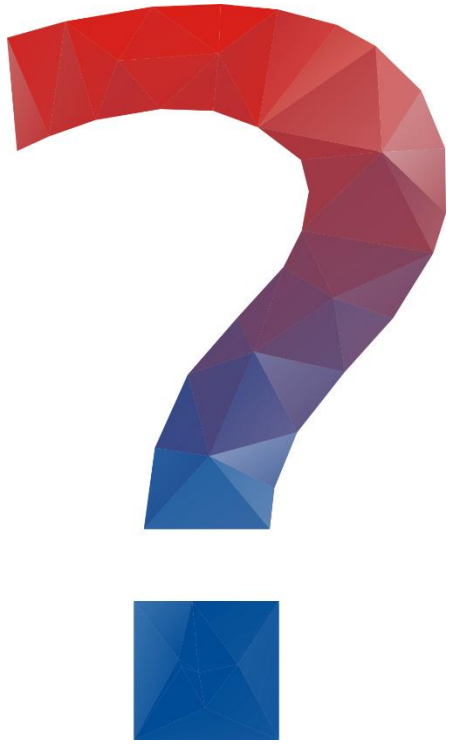
Supervisory instruments used

- Carrying out on-site inspections
- Developing a standard audit programme for "Cyber risk management"

Critical issues

- Taking into account security requirements to address critical service providers' cyber risks
- Increasing awareness amongst the Executive Board/Board of Directors of cyber risks (integrating cyber risks into the operational risk management)

finma



finma

THANK YOU!