



How Swiss Insurers are
Responding to Financial Crime
Insights from insurance leaders

October 2025

Contents

1. Introduction	
2. Regulators demand progress	3
The who and the where of risk	4
The dangers of life insurance	6
Old habits die hard	6
Outdated IT is expensive	7
3. Gen AI: game-changer	8
Tackling AI risks	9
4. Conclusion	11
5. Authors and contributors	14



1. Introduction

Within the financial sector, the insurance industry has traditionally been perceived as a bastion of stability, with a lower inherent risk of money laundering (ML) compared to the banking industry. This perception stems in part from the smaller number of insurance providers as well as the less frequent moving of funds in comparison to the banking sector. Nonetheless, the insurance sector does not remain immune to money laundering. Certain products present vulnerabilities that can be exploited for illicit purposes. Criminals continue to seek out ways in which to exploit insurance products and employ mechanisms to conceal the origin of illicit funds. Addressing crime effectively is not merely a matter of compliance; it is essential in achieving sustainable growth and competitiveness in the long-term. By recognising and addressing these risks, insurers can safeguard their integrity and contribute to a more secure financial environment.

To better understand and combat the risks posed to the industry by financial crime, Deloitte surveyed Compliance leaders in six insurance companies in Switzerland. The surveyed companies differ greatly in size, ranging from 5,000 to over 50,000 employees.

The survey aimed to gather insights into the current state of Anti-Financial Crime (AFC) functions within the Swiss insurance sector and to provide a view of Swiss insurance companies across several dimensions:

- AFC operations
- The main insurance product risks
- Regulatory challenges
- The cost of tackling AFC
- The role of AI in the sector's future.



2. Regulators demand progress

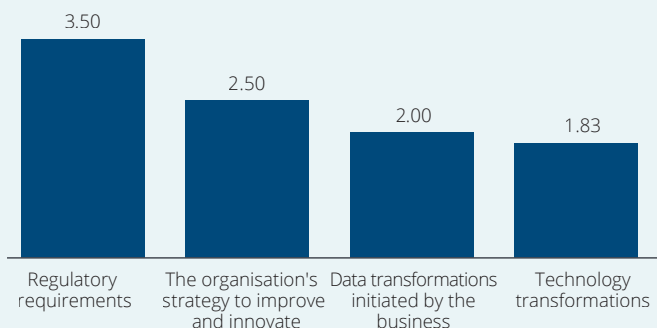
Heightened regulatory scrutiny is causing insurers to prioritise the fight against financial crime (FC). The industry also faces a pressing need to innovate and modernise in order to enhance the customer experience and improve efficiency and cost management in order to remain competitive.

As Figure 1 illustrates, survey respondents feel that regulatory requirements are putting them under most pressure to change. But regulators are by no means the only forces for change. Insurance companies want to innovate in order to address crime and are aware of the possibilities offered by more abundant data and new technologies.

These new tools are needed because the FC risks are becoming increasingly complex and unpredictable¹ and the insurance sector has to take a more agile and proactive approach. High quality data and advanced technology can combat FC threats and should be integrated into the business model.

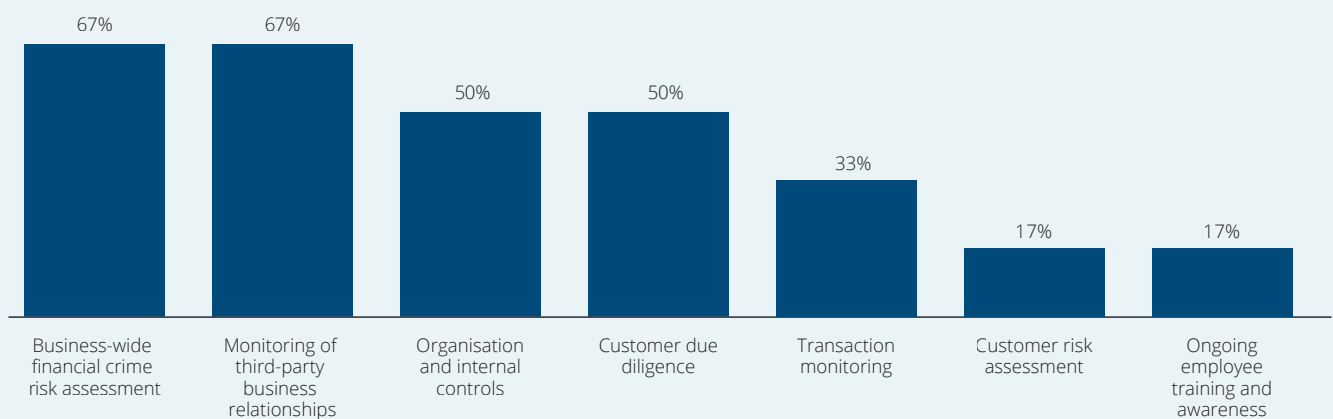
The survey indicates that most companies are implementing FC risk assessments, customer due diligence, and employee training. But integration with client lifecycle management processes is incomplete.

Figure 1. Average rating for what is driving change (1-5)



Source: Deloitte research

Figure 2. Most challenging measures to implement



Source: Deloitte research

¹ [Deloitte – 2025 Global insurance outlook](#)

The who and the where of risk

Pivotal to the fight against financial crime is a comprehensive understanding of the different risk categories, coupled with an assessment of those most critical to the individual insurance company. This evaluation is key to developing a targeted risk-based approach. In grasping the nuances and extent of exposure to various risk categories, such as customer, geographic, distribution/intermediary channel, product, and service and transaction risks, companies can tailor their strategies to effectively mitigate threats.

The extent of risk an insurance company faces depends on the products offered, distribution methods used, and payment acceptance processes employed. Although insurance companies are generally less vulnerable to money laundering than banks are, due to the partial obscuration of source of funds or beneficial owner, certain products such as life insurance remain vulnerable. Unlike banks, insurance companies do not provide current accounts, which limits their view of customer activity.

When evaluating various risk factors (see Figure 3), respondents consider customer risk as the most critical, followed by geographic risk. The degree of risk associated with different customers is far from uniform. Who the customer is, and where the customer is based, is critical. Insurers must, in their approach, prioritise scrutinising the riskiest customers and geographies: this is what is meant by a risk-based approach.

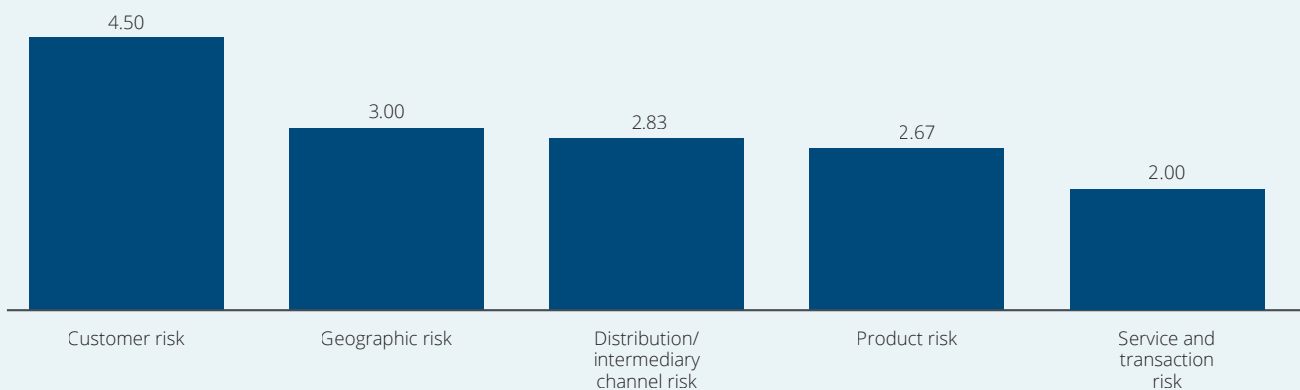
Distribution/intermediary risks, ranked third in importance, are challenging to address because the levels of organisational control and oversight vary widely.

Complex business structures can pose increased customer risk due to their ability to conceal ultimate beneficial ownership. Brokers prioritising sales over long-term retention or product suitability can lead to unsuitable sales and unnecessary product replacements² and hence increasing product risk.



Figure 3. Ranking of risk factors for ML/TF

Avg. importance on a scale from 1-5



Source: Deloitte research

² [150617-Draft-COB-Risks-Issues-Paper-for-consultation.pdf](#)

The dangers of life insurance

In high-value products such as life insurance, there can be obvious signs of risk. Among them are:

- single premium insurance policies: money launderers pour a large sum of money in a single transaction to protect illegally obtained funds
- relaxation periods: customers cancel their insurance coverage within a 14-to-30-day cooling-off period, allowing money launderers to receive a return before moving funds elsewhere
- annuities: money launderers can use their funds to pay for premium plans and earn monthly fixed cash flows
- policy payouts triggered shortly after signing up due to non-disclosure of serious issues that would have prevented the policy being signed
- unaware policyholders: policyholders do not know the policy has been set up. Detectable by analysing communication with the ‘customer’
- a spouse added as a beneficiary shortly before the policyholder suffers an “accident”
- abuse of the elderly – an older person pressured into adding an unrelated party shortly before a policy is redeemed
- payout details involving banks in non-cooperative locations outside the domicile of the policyholder.

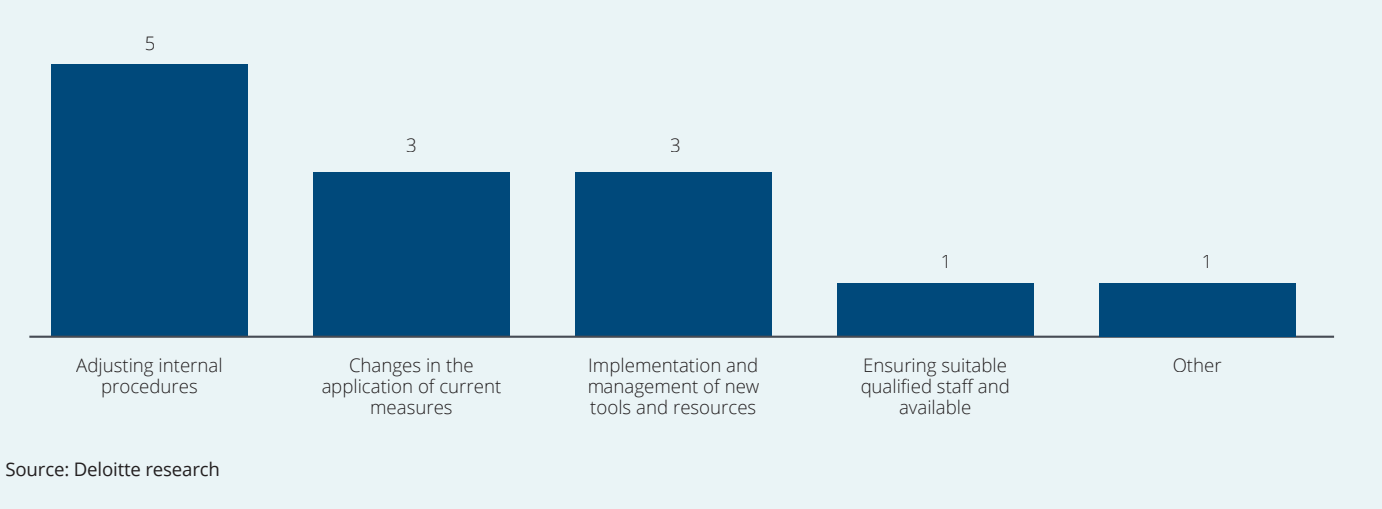
This demonstrates that, even when only considering life insurance products, the manners in which the signs of risk manifest themselves can be varied, posing significant challenges for insurers. In some instances, prompt actions may be taken directly, for example tracing policy payouts by bank compliance departments and filing Suspicious Activity Reports (SARs) swiftly in cases of suspected criminal activity. In other instances, certain incidents can lead to external action being taken independently from the insurance companies. Suspicious deaths of policyholders may trigger immediate law enforcement investigations, potentially subjecting insurers to heightened regulatory scrutiny where risk indicators having been overlooked.

Old habits die hard

Insurance industry regulation varies across jurisdictions and can exceed minimum standards in some locations. On money laundering, insurers generally adhere to the same regulatory requirements as banks, such as the EU’s 4th, 5th, and 6th AML directives, the U.S. Bank Secrecy Act, the UK’s ML and terrorist financing (TF) Regulations, and Switzerland’s AML Act and Ordinance.

To stay compliant, insurers must regularly adapt their AFC function. When asked about the new 2024 EU AML package, survey respondents indicated that their biggest challenge lies within changing their internal procedures. Old habits die hard.

Figure 4. Challenges implementing the New 2024 EU AML package



Outdated IT is expensive

Cost-efficient risk management is challenging. Employee costs and IT systems are the biggest expenses. Operational processes are often generic and manual and lack sufficient focus. This means that risk officers must spend a lot of time on repetitive tasks that could be automated.

Insufficient governance and accountability can also lead to duplicated efforts and delayed decision-making. The increasing complexity of new regulation and the growing frequency with which it is changed strains insurers' outdated IT systems, obliging costly workarounds that increase employees' workload. Third-party software licensing and maintenance is a significant added IT expense.

In financial institutions, the proportion of full-time employees dedicated to non-financial risk, including compliance, can reach up to 7% of the total workforce. Leading financial institutions typically average around 3%.³

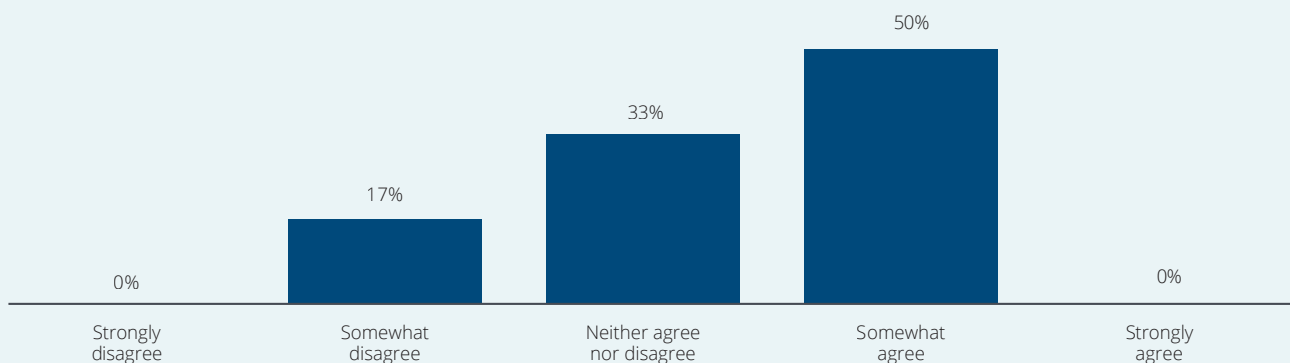
To address these challenges, insurers should revise their target operating model by adopting a risk-based approach.⁴ AI can be used to automate processing and focus resources on high-risk areas. Key strategies include centralised policy definitions, dedicated financial crime services, advanced technologies for automation and real-time monitoring.

Implementing such changes is costly but pays off in the future. Half of the respondents believe their organisation is devoting sufficient funds to combatting financial crime (see Figure 5). It is revealing that the companies which are satisfied with their budgets are spending less on average than those that are dissatisfied.



Figure 5. Budget adequacy

My organisation has sufficient budget to combat financial crime



Source: Deloitte research

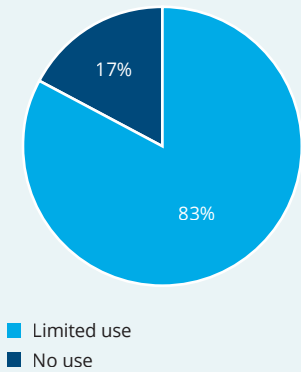
^{3 4} [Deloitte: Generative AI in Insurance](#)

3. GenAI: game-changer

Currently, the insurance industry's use of AI to fight financial crime is limited. As Figure 6 demonstrates, 83% of surveyed institutions reported limited use, while 17% indicated no use of new technology or AI in this context. Despite this and considering the technology's potential for the data-rich and language-heavy insurance industry is unmistakable, financial service firms have already made substantial investments, with \$35bn allocated globally in 2023. Projections by the World Economic forum indicate that this figure is expected to rise to \$97bn in annual investments by 2027, specifically with the sectors of insurance, banking, capital markets, and payments.

As figure 7 illustrates the vast majority of industry executives recognise the importance of AI, with one in two strongly agreeing that it will play a key role in fighting financial crime.

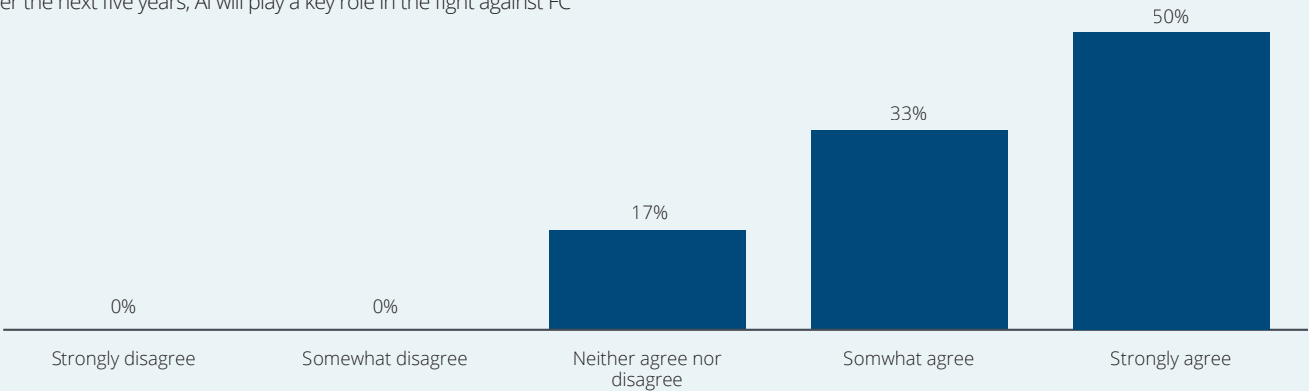
Figure 6. Use of new technology and AI in AFC



Source: Deloitte research

Figure 7. Future of AI usage in AFC

Over the next five years, AI will play a key role in the fight against FC

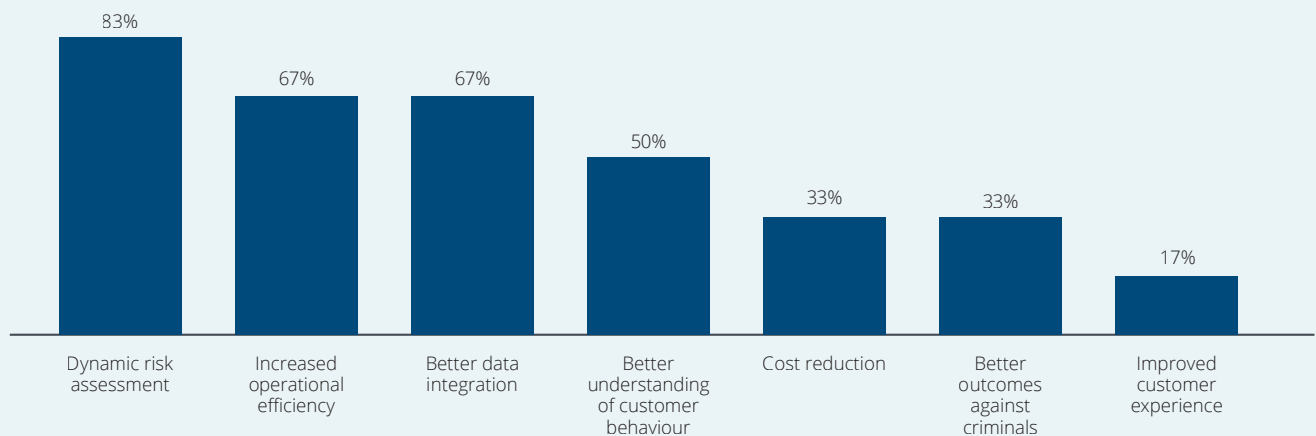


Source: Deloitte research

The industry expects AI to be useful in a wide range of areas (see Figure 8) where fighting financial crime is concerned. Dynamic risk management leads the list, with 83% of respondents expecting AI to enhance it. Automated data enrichment and tagging, generation of narrative for case notes from know your client profiles and intelligent triaging and prioritisation of alerts mean

that two thirds of respondents foresee advances in operational efficiency and in data integration, while half expect to enhance their understanding of customer behaviour. Harnessing AI for autonomous coding will accelerate the software development life cycle, leading to productivity gains and reduced training time, enhancing workforce productivity and operational intelligence.⁵

Figure 8. Expected benefits from AI in AFC



Source: Deloitte research

Tackling AI risks

AI presents risks of its own. The International Association of Insurance Supervisors (IAIS) identifies several risks associated with AI, including data privacy, bias, model risk, cybersecurity and concentration risk. It also highlights the complexity of AI and challenges related to accountability and traceability. An IAIS paper published in November 2024 aims to define clear governance around AI models to ensure robustness, safety and security while also promoting transparency and explainability.⁶

Many AI use cases remain conceptual because of the challenges involved in adapting legacy systems, which are labour-intensive, costly, and require specialist IT expertise (See Figure 9). All survey respondents say they lack the resources needed to implement AI and less than one-third of identified use cases successfully reach production.⁷

⁵ [Deloitte: Generative AI in Insurance](#)

⁶ [IAIS application paper](#)

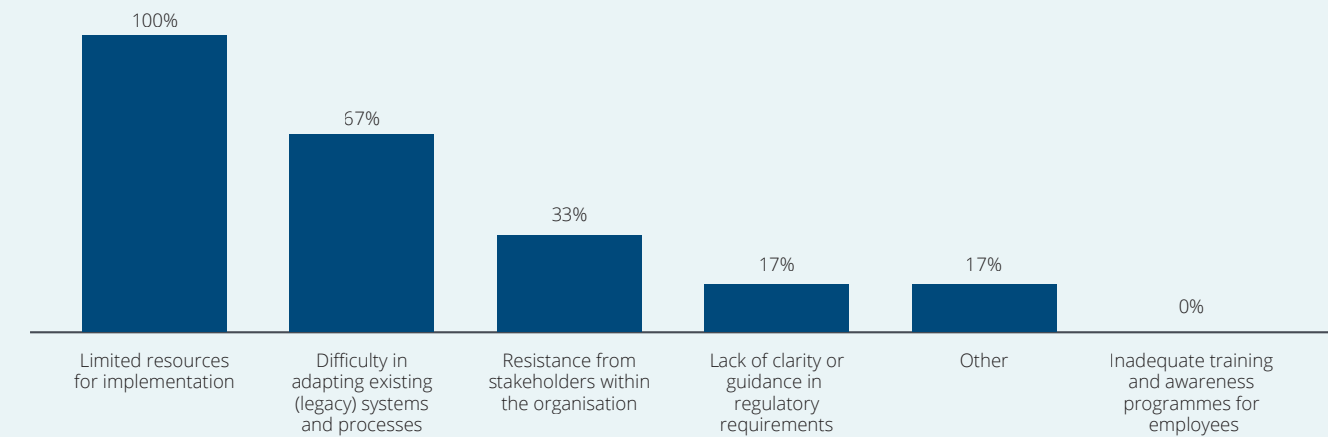
⁷ [13 Ways to Scale Generative AI \(and 9 Ways to Tell if You're on Track\) – WSJ](#)

Accessing accurate and high-quality data remains a significant challenge, as the survey indicates that few organisations automate customer relationship management feeds to enhance KYC data quality, resulting in error-prone, labour-intensive manual updates.

To overcome these challenges, organisations must develop a comprehensive strategy with a top-down mandate, focusing on high-impact and low-barrier use cases. Implementing repeatable processes and clear governance will help standardise and streamline work, ensuring stakeholder accountability throughout the development lifecycle. Engaging employees by documenting responsibilities and process changes will foster awareness and alignment for scaling and value creation. Prioritising flexible IT architecture and aligning data capabilities and processes with the AI strategy will ensure quality and accessibility.



Figure 9. Challenges when implementing change in AFC



Source: Deloitte research

4. Conclusion

The growing risks presented by financial crime, the increased costs of managing the risks, and the demands of regulators are forces of change in the insurance industry. The advent of new technology, AI and above all, Generative AI, offers means to successfully address financial crime while maintaining regulatory confidence and sector competitiveness. In order to tackle these challenges, insurers require a well-defined strategy.

Central to this is adopting a risk-based approach that devotes resources to the most significant risks. A risk-based approach focuses resources and efforts on higher-risk areas and customers, rather than applying a uniform strategy across all customers. In this way the costs of tackling financial crime can be reduced and dangers can be detected more effectively.

Insurers need to standardise their approach to financial crime, with centralised policy definitions, and they must deploy advanced technology and employ

dedicated financial crime services. Automation, real-time monitoring, and data analytics should be integrated into working processes to reduce manual efforts and enhance the accuracy of risk assessments. Employees must be educated about financial crime risks and shown how they can mitigate these risks. Incorporating a mechanism for continuous improvement is also essential given the rapid evolution of criminal tactics – and of regulation.

It is essential to recognise, as the vast majority of respondents to our survey do, that new technology and, in particular, AI offers promising solutions. AI can be used to reduce the reliance on manual labour and free up resources. It offers a way for insurers to progress rapidly in addressing financial crime. Insurers need to overcome the resistance to change and devote more resources to new technologies and AI-based solutions. Only in this way is financial crime likely to be tackled successfully and the industry's own future secured.



5. Authors



Uday Mehta

Partner
Risk, Regulatory and Financial Crime
udmehta@deloitte.ch



Michael Faske

Partner
Risk, Regulatory and Financial Crime
mfaske@deloitte.ch



Madan Sathe

Partner
Risk, Regulatory and Financial Crime
msathe@deloitte.ch



Philipp Lüttmann

Partner
Risk, Regulatory and Financial Crime
pluettmann@deloitte.ch



Michel Nyffenegger

Senior Manager
Risk, Regulatory and Financial Crime
mnyffenegger@deloitte.ch



Deloitte.

This publication has been written in general terms and we recommend that you obtain professional advice before acting or refraining from action on any of the contents of this publication. Deloitte AG accepts no liability for any loss occasioned to any person acting or refraining from action as a result of any material in this publication.

Deloitte AG is an affiliate of Deloitte NSE LLP, a member firm of Deloitte Touche Tohmatsu Limited, a UK private company limited by guarantee ("DTTL"). DTTL and each of its member firms are legally separate and independent entities. DTTL and Deloitte NSE LLP do not provide services to clients. Please see www.deloitte.com/ch/about to learn more about our global network of member firms.

Deloitte AG is an audit firm recognised and supervised by the Federal Audit Oversight Authority (FAOA) and the Swiss Financial Market Supervisory Authority (FINMA).

© 2025 Deloitte AG. All rights reserved.