Clarity on Financial Crime in Banking

Agility, risk and culture: three priorities for change

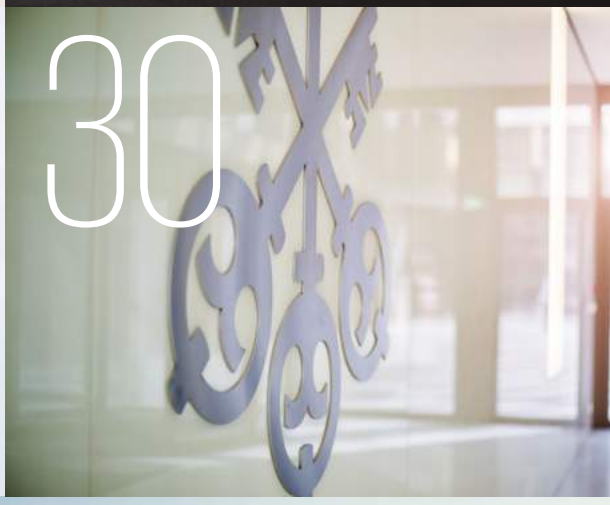
June 2018

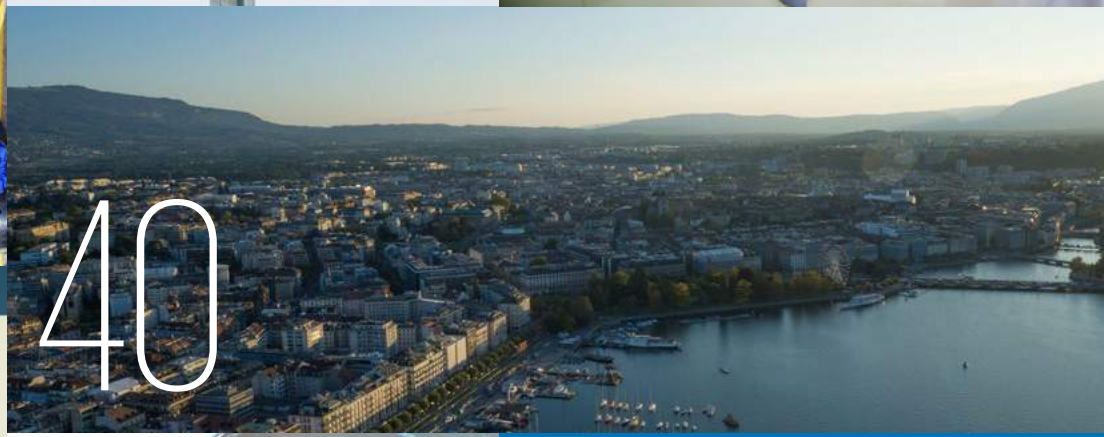
Ever-changing challenges
Internal line-up – The winning triad
- Structure
- Knowledge
- Compliance culture

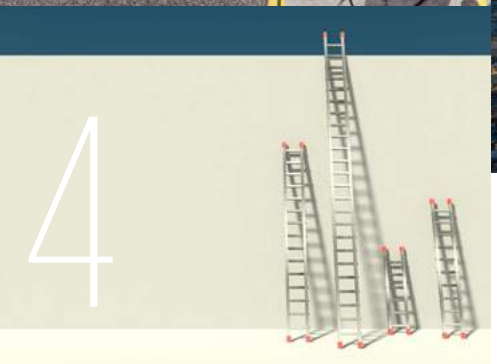
Joint Effort – the silver bullet for combating financial crimes

Interviews
Martin Peter, UBS Switzerland AG
Aurélien Dubus, BNP Paribas (Suisse) SA
Gemma Aiolfi, Basel Institute on Governance
Bernhard Hecht, Prosecutors Office of the Canton of Zurich
Daniel Tewlin, Former Prosecutors Office of the Canton of Zurich
Arnaud Beuret, Former MROS

Articles
Read our insights into how financial institutions can prevent and detect financial crime

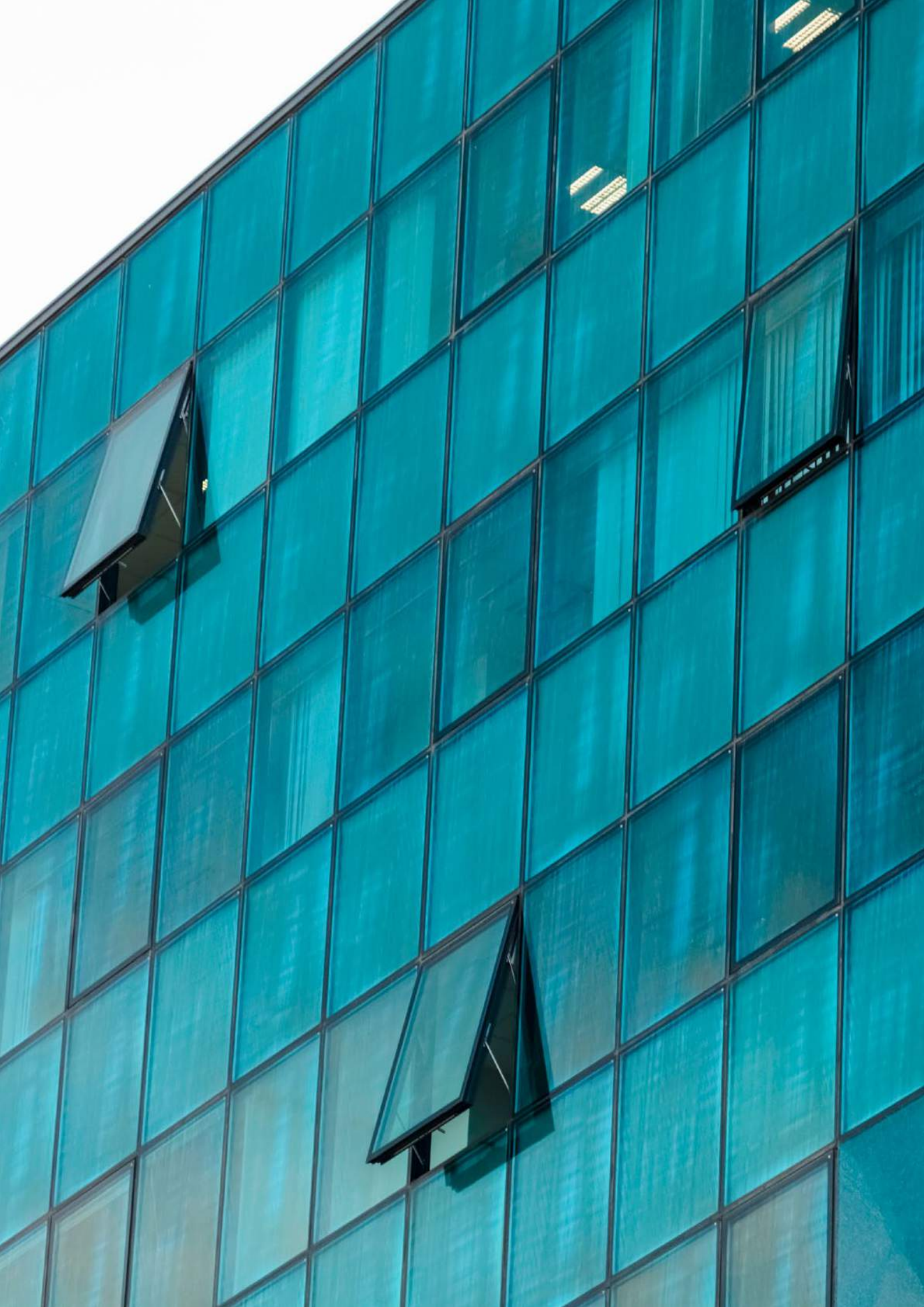






CONTENT

Clarity on Financial Crime in Banking



EDITORIAL

Agility, risk and culture: three priorities for change

Philipp Rickert
Partner, Head of Financial Services

Switzerland's role as an international financial center makes it uniquely exposed to financial crime, which in our digital age can emanate from anywhere in the world. Swiss banks and authorities face a huge challenge in preventing and identifying threats, to avoid being used as a financial hub for organized crime, money laundering and terrorist financing.

Government or state authorities would like to make financial intermediaries more responsible for this fight, and more accountable. They are prepared to do so through regulation. Specifically, they expect banks to play a preventive role, such as checking the involved parties as well as the origins of new money more comprehensively. This is no easy task given that money flows are difficult to track when they begin to cross national borders, and new technologies such as digital currencies mean offenders have more tools at their disposal to break audit trails and remain anonymous.

Criminals seem able to stay one step ahead, partly because of the reactive nature of regulatory development, and partly due to banks not sufficiently modernizing their risk approaches or IT infrastructures to clamp down on suspicious behaviors.

Banks must step up to the challenge. At present, too many Swiss banks' risk appetites are poorly determined, based on outdated inputs and suffering from a lack of effective implementation. Add to this the fact that many tools employed to protect the bank, its customers and society at large are no longer sufficient for today's and tomorrow's challenges. This includes inadequate transaction monitoring systems, a lack of rigor in customer onboarding such as KYC (Know Your Customer), and failing to make use of internal and external specialist support. This view is reinforced by our survey of 50 Swiss banks, the findings of which can be found in this publication.

Fortunately, there are many solutions at hand, and more to come. But banks must recognize the need for improvement. And in doing so, seek ways to collaborate with each other and with authorities to protect the reputation and health of the Swiss financial market.

As you reflect on how well equipped your organization is to combat financial crime, we hope you find this publication thought provoking. We would be happy to share with you our insights into how your bank can enhance the efficacy of its prevention and detection measures.

Philipp Rickert

Rising to the challenge

More precise, bank-specific risk assessments must become a priority, while qualitative improvements in areas such as client databases, transaction monitoring systems, and the use of artificial intelligence are central to enhancing the quality of alerts.

Too little, too late

When assessing the risk of financial crime, banks should consider primarily institution-specific factors when identifying high-risk countries, sectors or clients instead of relying on standardized public or purchased lists.


OP

Agility as prevention

Without investments in artificial intelligence tools, banks will increasingly struggle to meet strategic compliance objectives, reduce compliance costs and effectively manage regulatory changes. A better use of available tools is key to enhancing the dynamism of banks' compliance approaches.

The human factor

Greater investment in specialist support is needed to achieve the improvement in data quality and analysis necessary to better detect and prevent financial crime.

Sanctions support impact

The impacts of a bank's compliance culture and senior management 'tone at the top' will be diminished unless sanctions are enforced against employees who act in a non-compliant way.

Quality above all

By swamping the MROS with low quality notifications, banks could be limiting its ability to effectively filter and forward relevant cases to law enforcement agencies. It is critical that notifications are necessary, timely and appropriate.

Facts & Figures

Banks are impacted by financial crime in many ways. And their approaches to risk and the identification and prevention of crime can leave them exposed. The following charts demonstrate how Switzerland's banks have been affected by financial crimes over the past three years.

Financial crime the banking industry was used for in the last three years

22% **Money laundering**

12% **Identity theft**

11% **Embezzlement**

8% **Credit card fraud**

7% **Qualified tax offence**

6% **Market abuse/ manipulation**

6% **Bribery or corruption**

5% **Sanctioned transaction**

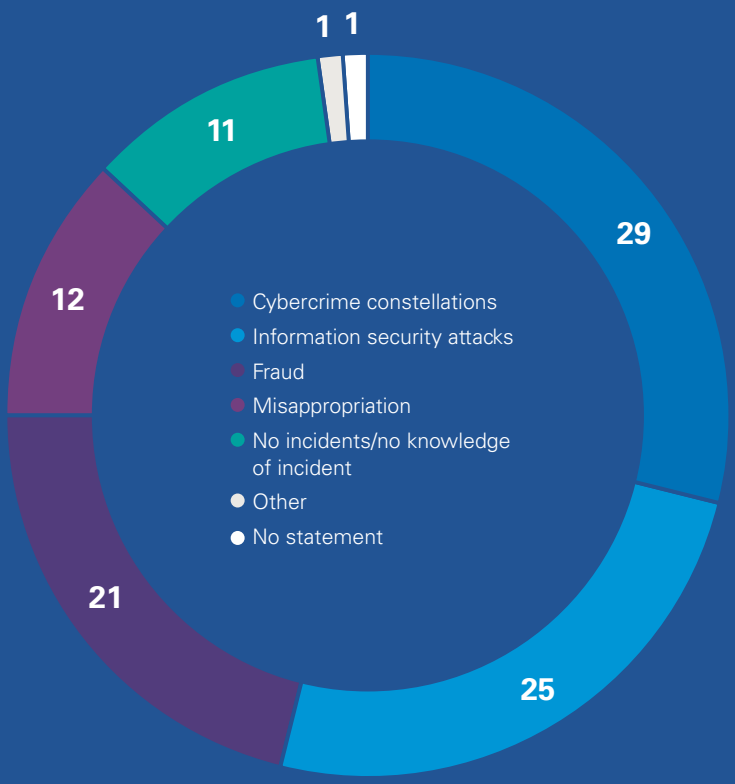
5% **Ponzi schemes**

3% **Other**

2% **Terrorist financing**

12% No incidents/ no knowledge of incidents
1% No statement

How banks were subjected to financial crimes in the last three years (in percent)



Who was the offender?

49% Offenders with no relationship to the bank

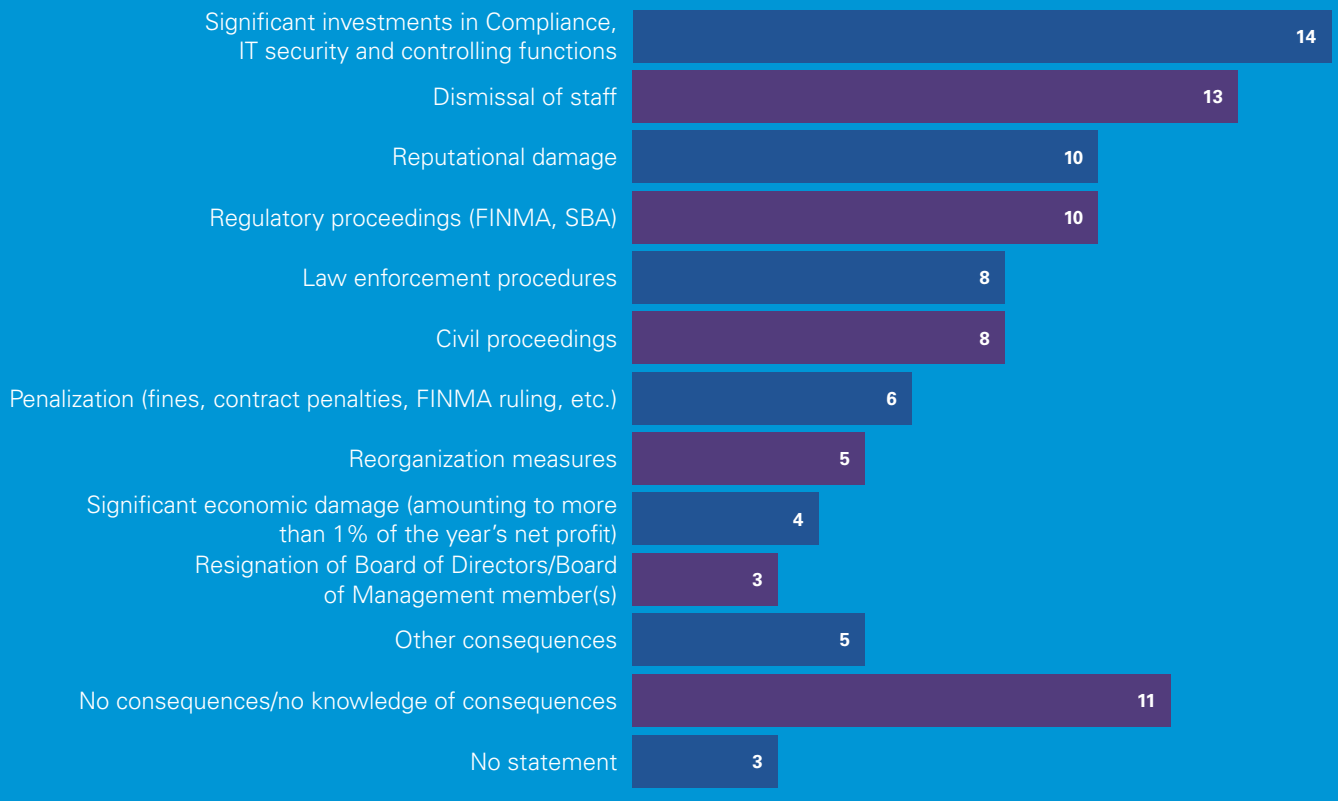
25% Staff members (current/former)

9% Third-party providers e.g. IT providers, consultants (current/former)

9% Clients (current/former)

8% No statement/ no knowledge

Consequences of being affected by financial crimes (in percent)



Key Findings

01 An underwhelming response to an overwhelming task: Swiss banks must rise to the challenge of detecting and preventing financial crime

02 Effective risk management in the context of prevention and detection of financial crimes requires professional, institution-specific approaches

03 Agility as prevention: building a dynamic approach and heightened employee awareness

04 The human factor: filling the gaps with specialist knowledge

05 Critical components for robust compliance: strong culture, tone at the top and an effective sanction system

06 MROS notifications must be based on quality

01

02

03

04

05

06

01

An underwhelming response to an overwhelming task: Swiss banks must rise to the challenge of detecting and preventing financial crime

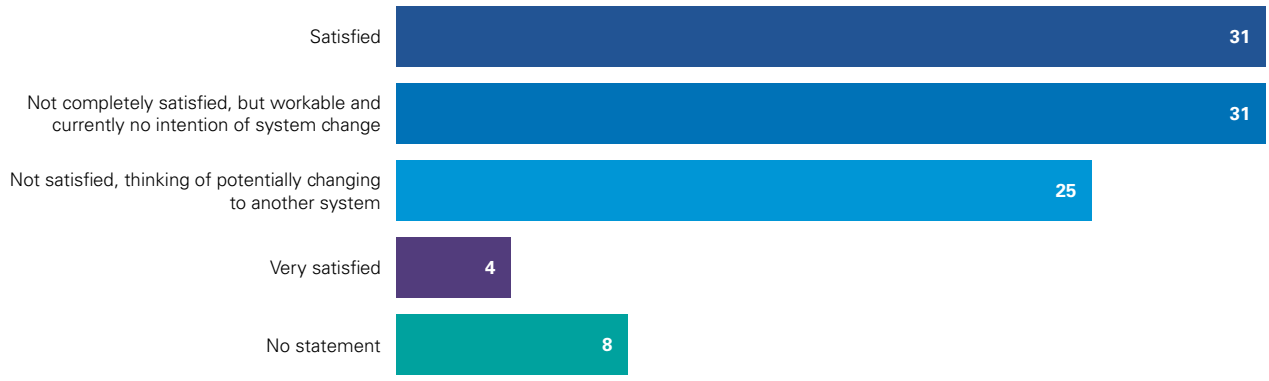
To better detect and prevent financial crimes, banks must carry out more precise risk assessments that take into account their specific business model. And develop tools to effectively implement their approach to risk as well as improving the quality of their client database. This may involve more effective calibration of transaction monitoring systems, or the use of artificial intelligence to enhance the quality of alerts and reduce the number of false positives. Without such measures, banks will continue to struggle.

Client assessments fail to consider transaction monitoring alerts and changes in the client relationship

CRM systems are not good enough at mapping customers. Information is often not updated and does not therefore reflect new risks in the bank's relationship with the client.

- One-quarter are dissatisfied with how their firm's CRM system maps customers and are currently thinking of potentially changing to another system
- One-third are not completely satisfied but expressed no intention to change the system

Satisfaction with CRM system with regard to the illustration of AML-relevant aspects (in percent)

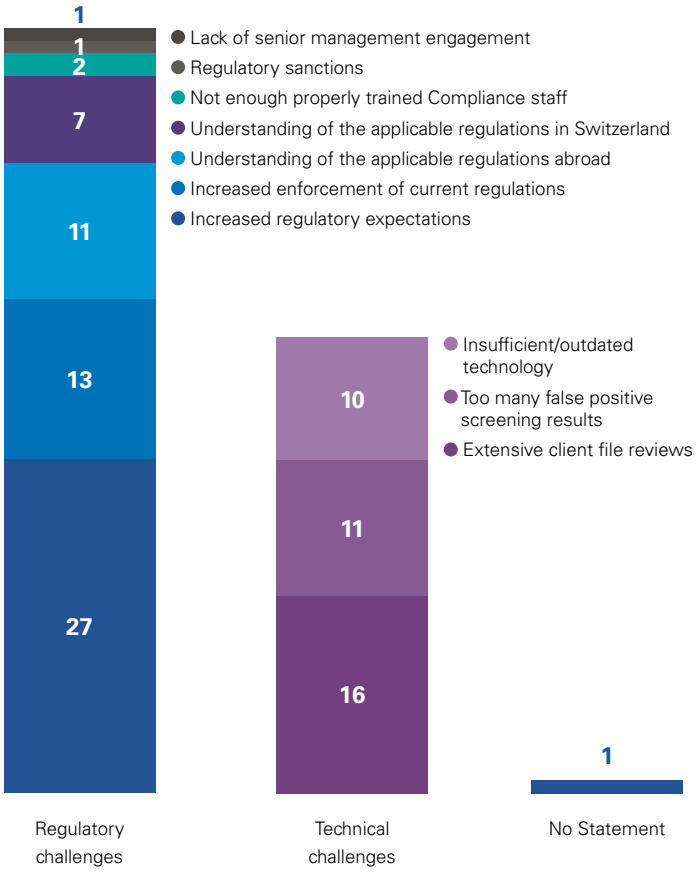


Current risk and transaction monitoring approaches are no longer sufficient for today's challenges

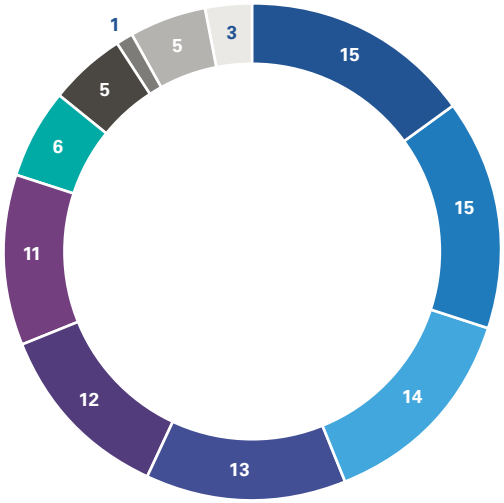
Banks often rely on standard risk methodologies, non-dynamic systems and outdated transaction monitoring approaches. The result is inefficient risk monitoring that yields too many false positives, as well as significant inefficiencies in both the first and second lines of defense.

- Only 12% of financial crimes are identified through transaction monitoring alerts
- Just half (52%) of banks are satisfied or very satisfied with their current client screening system with regard to comprehensibility, completeness and up-to-dateness of information provided. A further one-third are not completely satisfied but say their system is workable and there is no intention to change it
- 11% of the 50 banks say the biggest challenge they faced over the past two years has been too many false positive screening results

Major challenges banks were confronted with in the last two years (in percent)



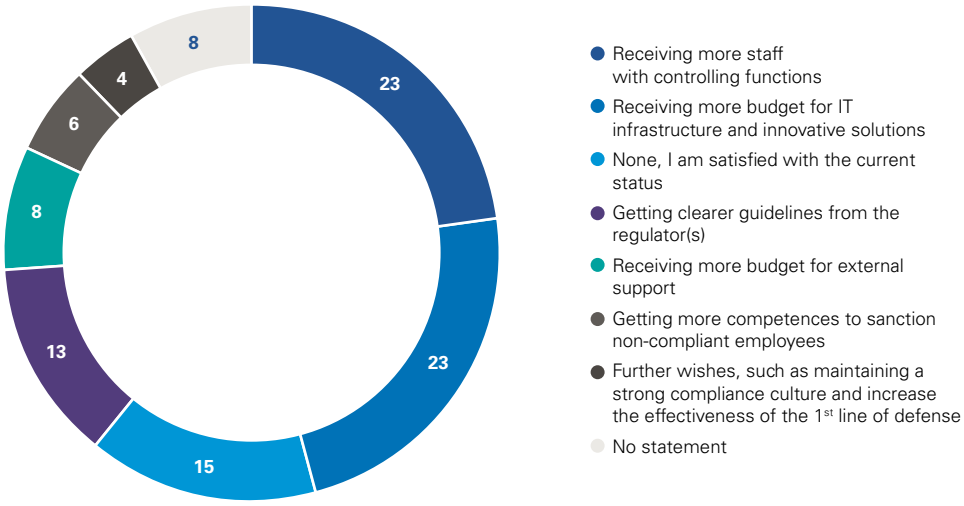
How did you become aware of being involved in/ targeted by a financial crime? (in percent)



External sources such as clients, media or authorities are too often the trigger for detecting financial crime

In 15% of cases, the organization was informed of the financial crime by a client, 13% by the media and 11% by authorities. The internal figures are no better: 15% of cases were reported by employees and only 1% by whistleblowers.

Wish list to efficiently master financial crime (in percent)



Greater investment in IT and human resources would generate only a small incremental benefit

- IT infrastructure and systems are often cited as priorities for investment. But given improvements already made, additional investment in traditional tools is unlikely to produce a relative increase in performance
- Investment is too often focused on the wrong areas, even in the views of bank respondents themselves
  - In terms of investments to overcome financial crimes, 40% of banks say investment at their organization is primarily in human resources, and 38% in IT and infrastructure
  - Only 23% feel that each of these is the most helpful area in which to invest. By contrast, 13% feel clearer guidelines from the regulator would be helpful, and 8% advocate a higher budget to secure third-party support

Clearer structures and processes are important to a successful and efficient Compliance function

As well as enhancing structures and processes, the detection or avoidance of financial crimes will not be optimized unless there is better information sharing and collaboration between Compliance and the Front Office.

Risk parameters are not regularly adapted to reflect current risks

Market developments might necessitate a more frequent and agile reevaluation of banks' core and non-core strategies and associated risks

Agenda for action

Banks need to do much more to effectively prevent and identify financial crimes, including:

- Establish the risk appetite regarding financial crimes, and define appropriate metrics for its measurement
- Acquire a better holistic understanding of the client and of his business activities
- Maintain current and up to date client documentation beyond what is formally required
- Secure prompt access to comprehensive data on clients and their business
- Keep good quality data and meaningful presentation of clients in systems, enabling the bank to gain an overall picture of its relationship with the client
- Appropriately calibrate transaction monitoring systems that is based on identified risks and business models, rather than the number of alerts
- Better use artificial intelligence to continuously improve the quality of monitoring

02

Effective risk management in the context of prevention and detection of financial crimes requires professional, institution-specific approaches

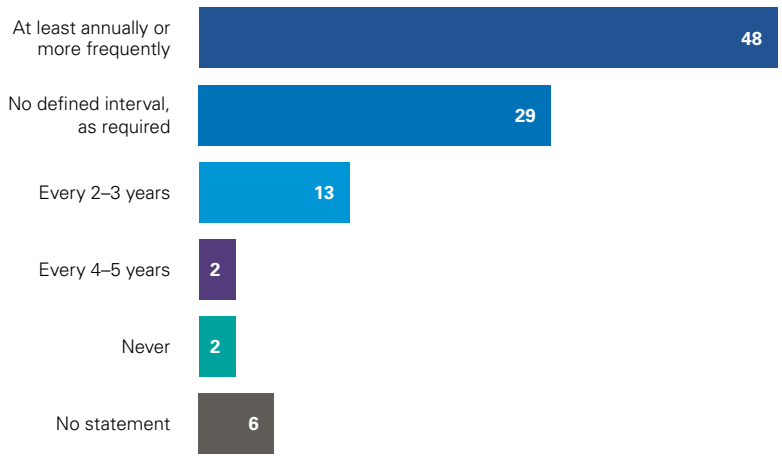
Some approaches adopted by Swiss banks to determining financial crime risks are inadequate. There is an excessive dependence on standardized public or purchased lists when identifying high-risk countries, sectors or clients. Institution-specific risks, including those that are particular to banks' own market, product and service features, are generally ignored. However, this requires a clear and comprehensive definition and implementation of institution-specific risk appetite, which is a challenge for all banks. This is where the Board of Directors must become involved.

Banks are too lax when reviewing their screening logic and system

Swiss banks are too relaxed when it comes to monitoring screening systems, and lack the system and processes to seamlessly adapt to sanctions updates. Action is needed regarding regular, systematic reviews of sanction screen logic, updates of sanctions lists, and transaction monitoring scenarios and thresholds.

- 29% review their approaches 'as required', not on a regular basis
- Fewer than half review their approaches annually or more frequently

How often do you test/review/audit sanction screening logic, updates of sanction lists, transaction monitoring scenarios and thresholds? (in percent)



The consequences of sanctions lists suddenly being amended are not always considered

- Sanctions lists can be amended quickly and without much warning, with the consequence that a banking client might suddenly represent a high risk to the bank. If banks do not anticipate changes to sanctions lists or do not act on changes immediately, the time lag between the amendment and the bank's action (such as blocking or terminating a client relationship) can expose the bank to risks
- Banks must continuously monitor amendments to sanctions lists and ensure their internal records are updated and reviews performed accordingly

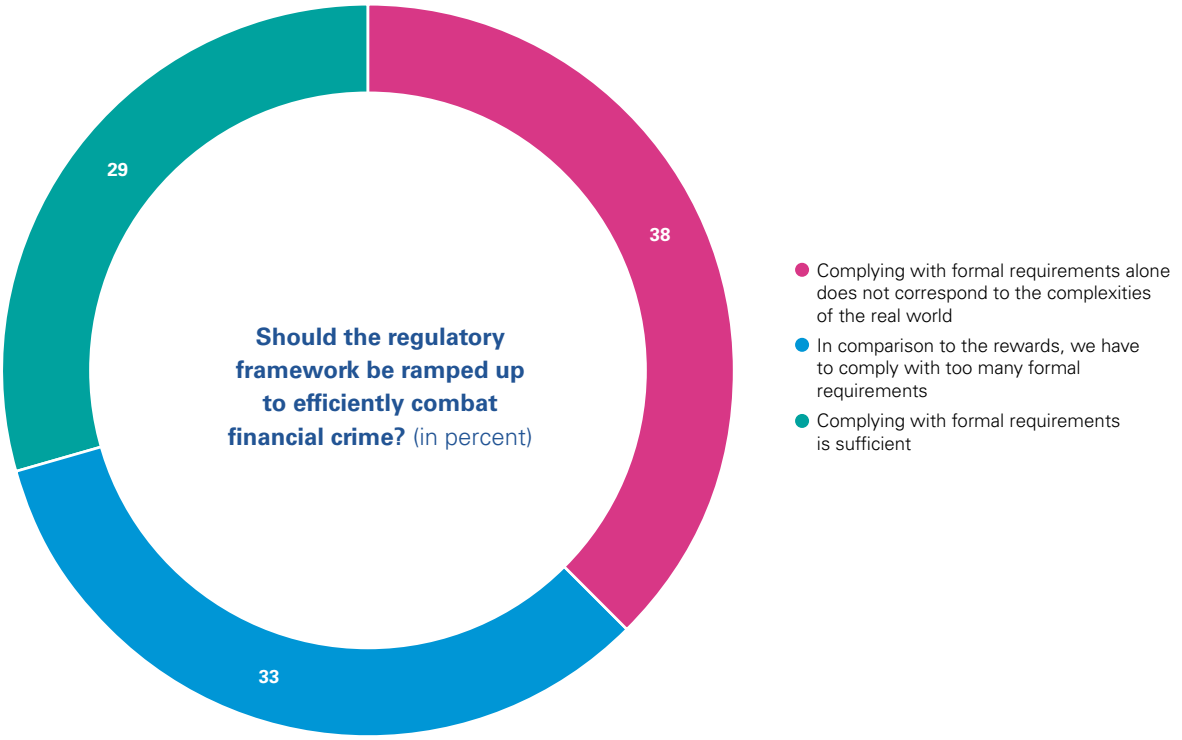
Institution-specific risk is hardly ever taken into account when defining high-risk targets

When assessing financial crime risk exposure, banks often do not take into account the institution's specific market, service offering and product strategies. As a consequence, the client information as well as related processes are not geared up to reflect the bank's ongoing risk appetite.

- 69% of banks assess product and service risks according to a combination of outdated key risk factors and individuals' own professional judgement
- Only 10% adapt public or purchased lists for high-risk countries to their own business and risk profile, and only 20% adapt lists of high-risk sectors

Too many banks believe compliance with basic regulatory requirements is sufficient

- It is not enough to comply with the minimum documentation required by regulations. Complex realities require consideration of many more factors if the combating of financial crime is to be effective
- An enhanced understanding of client transactions is key
  - 29% of respondents believe that complying with basic regulatory requirements is sufficient
  - One-third believe that they are obliged to comply with too many formal requirements relative to the potential benefits



Agenda for action

- Involve the Board of Directors in defining and implementing a comprehensive institution-specific risk appetite framework. As part of the bank's response to financial crime risks, this should include AML and sanctions risks inherent in the firm's specific markets, products and services strategies
- The Board of Directors must assign an adequate budget to implement appropriate risk measures to suit the risk appetite
- Ensure that the tone from the top drives the day to day living of the defined risk appetite, including greater ownership by the Front Office, to achieve effective risk mitigation
- Ensure up to date transaction monitoring scenarios and thresholds to combat money laundering
- Update sanctions lists at least once a week
- Consider the implications of newly issued or updated sanctions on the bank's business and clients
- Understand customers and their relationships with the bank, their business and transactions
- Check the plausibility of customers' transactions, including the underlying business rationale

EVER-CHANGING CHALLENGES: ARTICLE

Financial institutions and the combating of money laundering

Organized crime is on the rise[1]. And it is facilitated by tools such as money laundering. As ever tighter regulations come into force, and high profile corruption scandals embroil large financial institutions, why are banks and financial intermediaries still vulnerable to manipulation?

The process of laundering money to obscure its illegal origin can take several forms, from currency smuggling (physically transporting currency across borders), smurfing and structuring (depositing money in sufficiently small amounts to avoid triggering transaction reporting requirements) to so-called informal banking or 'hawala' (payments effected anonymously through a system of brokers). Whichever means is employed, it involves abusing or manipulating the financial system. Switzerland has witnessed its fair share of such problems in recent years, notably in connection with corruption scandals such as 1MDB and Petrobras. The repercussions for banks holding illegal money can be huge.

Regulation: always one step behind

Various regulatory obligations are already in place to prevent banks from enabling money laundering. The AMLA, AMLO-FINMA and CDB 16 impose specific duties of care on financial intermediaries. Notably, financial intermediaries must verify the client's identity, establish the beneficial owner's identity including sources of wealth and funds, clarify the transaction's economic background and purpose, and undertake further clarifications in the event of heightened risk.

One challenge with regulation, however, is that it can be out of date by the time it comes into force and presents challenges in practical application. This is because, firstly, regulation is too often a reaction to problems that have already caused adverse effects. And secondly, criminals have in the meantime developed new, more creative ways to achieve their goals. Cybercrime and cryptocurrencies are new challenges facing anti-money launderers, for instance. Authorities can do their best to ensure relevant regulations cover future developments (e.g. anti-money laundering measures referred to in Article 8 AMLA will automatically change with the realities of money laundering activities) but they may not provide intermediaries with sufficiently specific guidance.

Financial institutions: must do more

A second factor is the need for effective control mechanisms at intermediaries. In other words, financial firms must do more to ensure that regulations are effectively implemented. The Swiss Financial Market Supervisory Authority (FINMA) highlighted this issue while investigating the failings of banks in the 1MDB case. Heightened risks were insufficiently taken into account, incomplete and contradictory client information was left unquestioned, and plausibility assessments were not diligently performed.[2]

Financial intermediaries can counter these problems by investing in enhancing the effectiveness of their internal processes. The first line of defense lies in preventive measures. Risk and plausibility analyses should be continually adapted to address new risks and exposure. IT systems, internal guidelines and employee training should meanwhile be regularly evaluated and updated. The effectiveness of internal controls across the first and second lines of defense should also be continuously scrutinized.

Investing in the fortification of both lines of defense can help to ensure that financial intermediaries promote both the framework and the environment necessary to reduce money laundering risks. Because regulation and policy statements are not enough to remedy the vulnerability of Switzerland's financial institutions. The firms themselves need to better rise to the challenge.

[1] There has been a 45% rise in organized crime groups engaging in multiple criminal activities – a significant increase to the 33% rise in 2013. Europol Press Release, 9 March 2017

[2] FINMA media release, „FINMA informiert über 1MDB-Verfahren gegen J.P. Morgan", 21 December 2017

Money laundering and financial crime in the cryptocurrency age

Originally designed to circumvent the banking system for peer-to-peer transactions, cryptocurrency flows may in some ways be transparent and traceable, but recipients are identified only by an anonymous code. As criminals seek to exploit this weakness, how should financial institutions tackle this new way to launder money or finance terrorism?

The growth of cryptocurrency has gathered pace over the past ten years, and many financial institutions are only just starting to get to grips with this highly complex topic. As the blockchain underpinning cryptocurrencies does not typically store information such as IP addresses or personal data, it is it almost impossible for financial institutions to identify the beneficiary of an anonymous, numbered account. Banks can no longer rely on anti-money laundering concepts that worked for fiat currency (traditional legal tender). In an era of more and higher sanctions, this can be dangerous indeed.

Criminal options: money laundering through crypto cleansing

Crypto cleansing can be used to evade international sanctions. The typical cleansing process is as follows:

1. Purchase a cryptocurrency at a digital exchange or by cash or debit card at a digital currency ATM. The first is preferred as most crypto ATM providers are regulated. At a digital exchange, straw men with clean records and corroborated employment can be used. Pseudonyms strengthen their anonymity, as do anonymous e-wallets, log-less virtual private networks (VPNs) and blockchain-optimized smartphones.
2. Once the straw men are verified by the digital exchange, fiat currency or bank transfers are used to place funds to purchase primary coins. These are then able to purchase so-called alt-coins at an advanced exchange. Some alt-coins are privacy coins offering an increased level of anonymity.
3. Launderers use mixing (or tumbling) services to swap primary coin addresses for temporary digital wallet addresses to fool the blockchain and break audit traceability. Another tactic uses false receiving addresses to re-route transactions to backup addresses, also breaking the audit trail. Mixed primary coins are then transferred to an advance digital exchange to purchase privacy coins.
4. The next step is to layer multiple privacy coins, exchanges and digital addresses. After several layers, the audit trail can be severed, cleansing illicit funds to go back into the traditional financial system.
5. The money launderer can withdraw cleansed funds from the digital currency to fiat currency via:
   a. Burst-out integration: Privacy coins are changed to primary coins and later to a basic currency which can be withdrawn on a connected bank account or transferred to real estate, citing the desire to avoid capital gains taxes.
   b. Transfer of digital holdings to a hardware crypto wallet or printout of a QR code which can be transported to a desired addressee anywhere in the world.

Financial firms and regulators have various solutions at their disposal

AML procedures

For financial institutions, the higher risks should be addressed by reevaluating systems and processes in order to ensure they do not accept:

- flows from exchanges that do not require identification or KYC information
- proceeds of privacy coins (as far as this is detectable).

Transaction monitoring

The anonymity of cryptocurrency may prevent the financial institution from determining the beneficiary of a transaction, but IT systems can use algorithms to identify patterns and behaviors for fiat currencies to indicate existing money laundering schemes. And thereby identify accounts with possible links to criminal activity.

More focused regulations

Critics of cryptocurrency often say that the lack of identifying information throughout a digital transaction is a substantial obstacle to existing AML surveillance and enforcement capabilities. But in response, it is important to note that regulatory and enforcement elements such as identifying parties and information, or a record of the transaction, can exist in the world of cryptocurrency. At least in theory. Effectively containing the risks of cryptocurrency requires an expansion of worldwide KYC standards when issuing e-wallets.

As an international standard setter in the area of anti-money laundering, the Financial Action Task Force (FATF) in February 2018 leveraged work undertaken by South Korea's Financial Services Commission on anti-money laundering compliance rules for domestic cryptocurrency exchanges. They looked at the South Korean ban on anonymous trading accounts, and a new requirement for exchange platforms to perform real name verifications. Anonymous or pseudo-named wallets are no longer permitted in South Korea.

Third party ID providers

To guarantee a certain degree of anonymity for law abiding citizens, while allowing authorities to pursue criminal elements, third party ID providers may be key to avoiding burdensome identification and KYC data collation.

Regulate advanced digital exchanges

Regulating exchanges that offer primary currency is easier due to the fact that they often accept fiat currency in exchange for a primary cryptocurrency such as bitcoin. However, the focus should also be on regulating so-called advanced digital exchanges that only offer exchange from primary coins to alt coins. Regulating such exchanges could be useful as, while a privacy coin's audit trail might be anonymous, the digital exchange is able to view its own trades and digital wallet balances.

Better use of blockchain

Blockchain technology inherently has the potential to reduce AML risks compared to fiat currencies. Blockchains maintained via an online public ledger means each transaction can be supervised, validated and recorded in a complete history. Also, cryptocurrency is almost impossible to forge as each type carries unique characteristics, which are verified from end-to-end miners. Without verification of all transaction phases, including the departure wallet, destination walled, currency type and amount, the transaction would be immediately blocked without any human involvement. In this sense the digital trail could better serve AML than an existing fiat paper trail. In addition, it is technically feasible to revise the blockchain protocol to limit transactions to KYC–verified wallets. Further AML risk analysis and alert and reporting mechanisms could also be integrated into the crypto system.

Ultimately, the most effective approach is likely to be a combination of these considerations. Regulators must develop more up-to-date, focused standards that deal with the challenges of this rapidly evolving area. And financial institutions must take responsibility for ensuring their systems and processes are capable of mitigating the risks insofar as possible. In doing so, all parties could utilize latest technologies such as blockchain to take the fight to the financial criminals.

Large-scale challenges: multinational banks and prevention of financial crime

The answer to tackling financial crime is not to expand the Compliance function. Extra budget and headcount can take you only so far. The answer is to educate and empower employees to identify risks in a broader range of issues, from IT security to cyber crime. Martin Peter, Head of Compliance & Operational Risk Control and member of the Executive Board, UBS Switzerland AG, shares his thoughts on the particular challenges facing a large bank in addressing crime.

Martin Peter, Head of Compliance & Operational Risk Control and member of the Executive Board, UBS Switzerland AG.

«We are a second line of defense function, controlling and guiding the business and critically questioning its decisions.»

KPMG *You have held various legal and compliance positions at UBS for over 20 years. How have the functions' responsibilities evolved over this time?*

Peter In the beginning, Compliance was part of the Legal function. Over time, the growing legal and regulatory expectations and changes mean the Compliance function has evolved and grown in size and importance. Initially Compliance used to focus primarily on Know Your Customer and anti-money laundering issues, focusing on training and advising client advisors. More granular advice was needed in private banking, and to some extent corporate banking. Today, we have evolved into an independent control function that identifies the regulatory requirements and ensures that Compliance risks are understood, owned and managed appropriately. We are a second line of defense function, controlling and guiding the business and critically questioning its decisions.

Whereas in the past we were primarily concerned with financial crime, today we deal with a much wider range of key topics and a wider range of activities. Topics range from anti-money laundering, suitability, cross border or conflicts of interest to IT security and protection against cyber crime, or regulatory reporting. This has an impact on the skills set required of employees. As a consequence, employee profiles range from a legal background to banking specialists or IT and data mining experts. More and more employees in the Compliance department are highly specialized. The generalist Compliance Officer is becoming less and less common at large banks.

We see senior management, employee behavior and culture having a direct influence on how effectively a bank fights financial crime. Is that consistent with your own observations?

Most important is the tone from the top. Top management sets the principles and practices how we do our business and defines the bank's risk tolerance, compliance and anti-money laundering, sanctions, etc. programs. In addition, senior management ensures implementation of the standards and rules by providing the appropriate resources and support. This includes the adequate handling of compliance failures. A careful balance must be applied between acceptable fault tolerance, consistent intervention and avoidance of a fear culture. I am of the opinion that behavior in line with Compliance requirements must be rewarded. For example, if a client advisor loses a client as a consequence of compliance with his or her reporting of an incident.

Is investment in IT tools a key driver of efficiency or are other factors more important?

The question is do we detect more money laundering-related circumstances through more automated and more efficient tools? In my view,

this could only be achieved through tools which have the ability to learn without being explicitly programmed. In recent years, we have made great progress towards continuous real-time monitoring. However, few violations of the Money Laundering Act were uncovered by these monitoring measures. The regulator and the industry had certainly expected more out of this. Either the parameters are set incorrectly or the money we receive is actually clean and satisfies stringent prerequisites.

How do you sensitize your employees to look out for and recognize new crime scenarios?
Taking into account that Compliance employees are highly specialized and participate in various working groups we share this knowledge within the Compliance function and across the business by providing continuous classroom and web-based trainings. Our client advisors are continuously trained and educated. In addition, we make available continuously updated factsheets and Q&As on new topics such as cryptocurrencies. And we have regular meetings with senior management and other risk functions where new developments and challenges are being discussed. Meanwhile, specific warnings or briefings are given to specific target groups in a personal exchange.

Which of a bank's products and services do you believe pose the greatest risks?
From an AML perspective, client activities - be it on a transactional, product or counterparty level with the potential for less transparency. For example physical cash transactions, precious metal transactions or virtual currencies pose a higher risk. And, of course, there are customers from certain regions and countries or in sensitive industries who bring a very different risk profile compared to a Swiss salary account holder.

What challenges do Swiss banks see themselves facing in the fight against money laundering, terrorist financing, etc.?
In Switzerland, we manage substantial amounts of assets of foreign clients, which increases the effort required for the ongoing monitoring of these client relationships. Switzerland still suffers from the slightly tarnished image as a hotbed of black money, which continues to drive foreign regulators to keep a close eye on Swiss banks. Ultimately, as a bank, you simply have to be clear about the additional costs involved in looking after a customer from particular countries or industries.

When identifying potential money laundering cases, is the challenge to understand your customer/KYC documentation or to analyze payment flows?
The due diligence measures, being the basis for the KYC documentation, applied by the client advisors are linked to the risk potential of a specific client relationship. The different due diligence levels might include client contact, additional screenings of publicly available sources as well as potentially via reliable third party sources where necessary. This is complemented by further monitoring steps on a transactional level, which, depending on the client activity, volume and transactional pattern can be very challenging. The combination of all measures aims to prevent and detect suspicion of money laundering including corruption and terrorism.

We asked our survey participants what they would like to improve the fight against financial crime within their institution. Most wanted more human resources or a higher budget. What would be your wish for UBS?
Although more resources and a higher budget might sound tempting, our main goal remains to ensure through our interaction with the business at all levels and the programs in place that the inherent compliance risks are correctly understood, managed and owned accordingly. To this end, and in support thereof, more resources or budget in the right place can definitely be a means to achieve this. Notwithstanding the resources to hand (human or sophisticated tools supporting the programs in place) the industry faces challenges in the sometimes differing expectations from the various Swiss authorities in charge, the changing environment in the money laundering reporting regime as well as applicable rules leaving room for interpretation.

Additionally, an improved exchange of information between authorities and the private sector would be desirable. It appears that some government agencies have more detailed information about our customers than we have. But this wish will probably fail due to ever stricter data protection provisions.

03

Agility as prevention: building a dynamic approach and heightened employee awareness

Increasing Compliance dynamism and investing in artificial intelligence (AI) tools is critical to meeting strategic compliance objectives, reducing compliance costs and effectively managing regulatory change.

A dynamic approach enables swift and appropriate action as the environment evolves

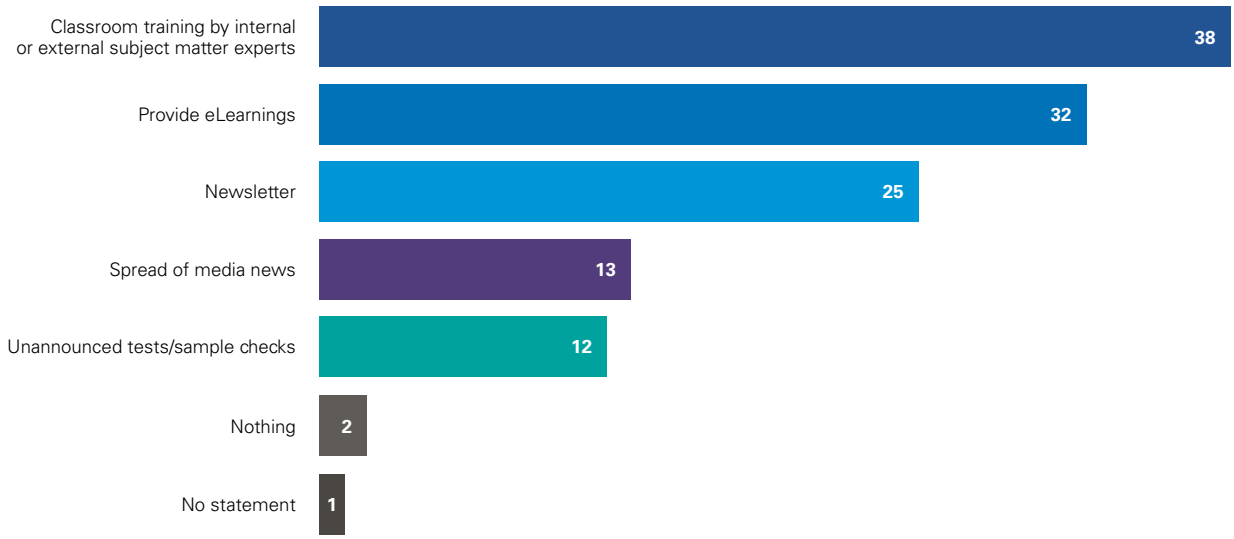
- Ongoing changes to the regulatory environment, and advances in technology and criminal sophistication, mean Compliance must remain agile if it is to adapt and respond quickly
- Compliance functions that apply AI tools and have access to specialist teams will be the most agile

Timely and targeted knowledge sharing within the bank reduces exposure

If employees are not aware of the latest types of financial crime that could affect the bank, incidents are more likely to be successful. Prompt communication is therefore key. This can be delivered through classroom training courses and eLearning, as well as other forms of internal communication such as newsletters, intranet and email.

- The use of classroom training courses and eLearning at banks is widespread
- Only half of respondents issue internal newsletters to raise employee awareness of new types of financial crime, however, and one-quarter share news from the media

What does your bank do to sensitize employees to new financial crimes?
(number of banks, more than one answer possible)



Agenda for action

- Tailor investment in Compliance to precise regulatory changes for a more focused outcome
- Use AI tools to increase efficiency and cost-effectiveness in combating financial crime
- Ensure that intelligence automation is designed and implemented by specialists, whether in-house or external
- Combine learning channels to raise awareness among employees of new types of financial crime

As easy as ABC? Strengthening compliance amid regulatory scrutiny

Robust internal frameworks are needed to counter the risks of financial crime. But while anti-money laundering measures help to defend against being used to forward crime proceeds, not all threats are external. Banks are also exposed to financial and reputational damage from corrupt conduct by their own employees and associated third parties. As scrutiny by local and foreign authorities intensifies, what principles should guide effective internal policies and procedures to avoid censure?

Recent years have seen governmental and non-governmental authorities around the world provide more concrete guidance on the measures needed to deal with financial crime risks. This is especially notable in the case of anti-corruption and bribery (ABC). We discuss some of the primary guidance.

Wolfsberg Group: ABC Compliance Programme Guidance

The Swiss-based Wolfsberg Group is a non-governmental association of thirteen global banks. In June 2017, it released its "Anti-Bribery and Corruption (ABC) Compliance Programme Guidance". Given the key role played by the financial services industry in the fight against bribery and corruption, the guidance is intended to support the development, implementation and maintenance of effective ABC compliance programs.

The guidance emphasizes the importance of a risk-based approach. It also covers a range of internal measures financial institutions should take to reduce corruption by their own employees as well as third parties conducting business on their behalf. Breaking down the key elements of an ABC program, it addresses:

- governance, including recommendations regarding the allocation of roles and responsibilities, internal reporting and independent review
- firm-wide policy, reflecting zero tolerance for bribery and similar facilitation payments, with senior management setting the tone from the top
- measures to manage risks from third-party providers
- gifts and business hospitality
- risk assessment
- training
- compliance monitoring.

The Wolfsberg ABC Guidance explicitly draws on issuances by the UK Ministry of Justice (MOJ), the US Department of Justice (DOJ) and the US Securities and Exchange Commission (SEC).

UK: MOJ guidance on the Bribery Act

In the UK, corruption in the form of bribery is prohibited by the 2010 Bribery Act. As well as the general offenses of active and passive bribery, a specific corporate bribery offense holds commercial organizations accountable for failing to prevent bribery. An organization can be exonerated, however, if it can prove it has adequate procedures in place to prevent associated persons from engaging in bribery.

More detailed information about such procedures is provided in the 2012 guidance published by the MOJ.[1] It sets out six principles to aid commercial organizations in their financial crime management processes, such as the proportionality of procedures, top-level commitment, risk assessment, due diligence, communication, and monitoring and review.

[1] "The Bribery Act 2010 – Guidance about procedures which relevant commercial organisations can put into place to prevent persons associated with them from bribing (section 9 of the Bribery Act 2010)", Ministry of Justice, 11 February 2012

US: DOJ and SEC guidance on the FCPA

A similar set of guidance principles was published in the US in 2012 as a result of a collaboration between the DOJ and the SEC based on federal anti-bribery obligations set out in the Foreign Corrupt Practices Act of 1977 (FCPA).[2]

The guidance highlights the following principles as hallmarks of effective compliance programs: commitment from senior management and a clearly articulated ABC policy; code of conduct and compliance policies and procedures; oversight, autonomy and resources; risk assessment; training and continuing advice; incentives and disciplinary measures; and third-party due diligence and payments.

While there is no explicit statutory defense in the FCPA as there is in the UK Bribery Act, the DOJ and SEC take into account the adequacy of a compliance program when deciding if and what action to take against an organization. It may also affect the penalty imposed in the event of wrongdoing.

France: AFA guidance on Sapin II

A more recent development in this regulatory trend is the guidance[3] provided by the Agence Française Anticorruption (AFA) on "Sapin II", France's new anti-bribery law that requires firms to establish an anti-corruption program to identify and mitigate corruption risks. It contains elements that are reminiscent of the principles in its UK and US counterparts. It also covers the subjects of top management commitment in setting a zero tolerance policy for corruption risk, content, scope and form of an anti-corruption code of conduct, third-party due diligence procedures, corruption risk training and an internal monitoring and assessment system.

In addition, it highlights the importance of an internal whistleblowing system as part of an ABC Code of Conduct for employees to report activity that may be in breach of the company's code. And detailed information on risk mapping as the foundation of a risk management strategy.

In agreement: a flexible and tailored approach is key

Despite some variations, all three sets of guidance provide similar guiding principles and specific recommendations to help businesses set up and maintain effective ABC compliance programs. Because they emphasize a flexible and tailored approach – as opposed to a 'tick the box' solution that may not make sense for every financial institution – they offer an adaptable road map for setting up internal structures and processes.

With the financial services industry being so strongly interconnected, it is more important than ever for firms to ensure compliance with all relevant laws and regulations. These sources of guidance represent elements of an international consensus on compliance best practices. As such, they should be considered by Swiss financial institutions.

In short, the right compliance framework, efficient and clear processes to ensure it is implemented correctly, and the promotion of a culture of compliance across all functions are all critical elements. They will not only help financial institutions minimize their exposure to financial and reputational losses from bribery and corruption, but also strengthen trust in the highly competitive financial services sector.

---

2 "A Resource Guide to the US Foreign Corrupt Practices Act", DOJ/SEC, 14 November 2012

3 "Guidelines to help private and public sector entities prevent and detect corruption, influence peddling, extortion by public officials, unlawful taking of interest, misappropriation of public funds and favouritism", AFA, Version 12-2017

Innovation in compliance: the importance of artificial intelligence

Automating compliance programs can help businesses address financial crime and AML. In particular, it supports efforts to meet strategic compliance objectives, reduce compliance costs, and ensure effective implementation of regulatory change. So which areas should banks focus on to achieve these goals?

An entire spectrum of innovation can help to combat financial crime. Not least, new and evolving forms of artificial intelligence (AI). Among the primary examples that banks could make use of are:

- **Robotics Process Automation (RPA):** this entry point to automation relates to programming software to perform highly repetitive tasks. The use of RPA allows humans to focus on higher value tasks and dedicate more of their time to areas of greater potential risk.
- **Machine learning:** software algorithms that are not explicitly programmed and that can predict outcomes or draw inferences based on input data. It is one of the main components that drive predictive capabilities and is a core foundation for cognitive systems.
- **Cognitive:** a self-learning platform that mimics the attributes of human reasoning and decision making while interpreting far greater volumes of data than is humanly possible.

Whether these technologies are adopted individually or together, they must form part of a pre-determined AI strategy that underpins the organization's efforts against financial crime. Such a strategy should be based on what investment the institution is willing to make and what benefits it seeks. This includes weighting the potential risk involved against the efficiency and agility desired. So that the result is an AI strategy that is aligned with the size and scope of the institution and its risk tolerance.

Three key areas where AI could be of use

We set out three areas of consideration where AI can help banks in the fight against financial crime:

Transaction monitoring

- **RPA:** Save analysts' time by employing bots to scan the internet and specified public due diligence (public database) sites as well as collect relevant data from internal sources and acceptable third party sources (as identified by the institution).
- **Machine learning:** Machines can be used to automate aspects of the review process. They can build statistical models based on gathered data to calculate a likelihood for disposition, either closing or escalating a case. Significant efficiency gains can be made in automated alerts together with a rationale for the decision to be taken
- **Cognitive:** Builds on existing alerts and cases, together with the bank's machine learning. Cognitive does not rely on an institution's underlying rules-based transaction monitoring systems. Instead, it enhances machine learning models already in place to provide a domain knowledge base on which the cognitive platform can rely. Because the tool does not limit its monitoring to known risks, but rather looks at patterns in the data, it is key to finding new and emerging financial crime risks.

Know your Customer (KYC)

- **RPA:** As KYC processes tend to compromise highly repetitive tasks, many banks have identified areas where RPA can save significant time. As robots may achieve greater accuracy in due diligence information collected, RPA could result in a better customer experience by reducing or eliminating the need to contact customers repeatedly.
- **Machine learning:** Can be implemented to automate the reading and extraction of data from unstructured documents. Coupled with RPA, the customer risk rating process can be more reliable and more efficient. This enables banks to move closer to real-time risk assessment, and a more accurate analysis of customers' current risks.
- **Cognitive:** With RPA and machine learning solutions in place, cognitive can apply judgement based on the domain knowledge base (e.g. identify the most relevant articles) and identify KYC outliers that are possible risk indicators. This allows the bank to better prioritize its KYC efforts and means the information obtained better reflects actual risks, along with a robust analysis audit trail.

Compliance testing

- **RPA:** Can help to quickly identify issues from initial datasets for review by humans as part of their testing scope work. Depending on how structured the data are, RPA could be used to conduct basic testing procedures to identify data completeness (e.g. examine all KYC files for inclusion of required data points such as address, date of birth, citizenship, source of wealth, etc. in accordance with the bank's protocols).
- **Machine learning:** Can be used to ingest structured and unstructured data and rely upon a library of test steps to automatically assess the data. This would be read by machine and any identified exceptions reviewed by humans.
- **Cognitive:** Using prior outcomes from compliance monitoring and testing, internal audit activities, regulator investigations, enforcement orders and other public information, the domain base knowledge of financial crime compliance can be built and applied to the bank's customers, products, services etc. to search for patterns and to compare those to the built domain base knowledge. This allows the identification of issues that were not items that failed a particular test, but rather outliers that require assessment by a human to evaluate potential risk.

The potential for banks to better use AI to meet their compliance objectives – in a more efficient and effective way – is clear. But investment is required to gain access to the most appropriate technologies, tailored to the bank's needs. It is imperative that banks keep an eye on this rapidly evolving area, as new and emerging technologies arise that can add even greater value to the bank's fight against financial crime.

Investment in Compliance: preserving the bank's long-term value

With around 1,500 employees across branches in Geneva, Zurich, Basel and Lugano, BNP Paribas (Suisse) SA is a leading European bank for companies, institutions and private clients in Switzerland. Aurélien Dubus, Head Compliance, shares his insights into compliance risk management and how to build specialist competences to be able to manage the unexpected.

Aurélien Dubus,
Head Compliance
BNP Paribas (Suisse) SA

KPMG *Increasing regulatory requirements are resulting in longer file processing times. What measures are banks taking to handle workflow while complying with regulatory requirements and cost constraints?*

Dubus Compliance processes involve reconciling qualitative and quantitative objectives. To achieve this, financial institutions must focus on three priorities:

1. The Compliance function must continue to become more professional, strengthening Compliance Officers' expertise, in particular through increasingly advanced training.
2. There is a growing awareness of the compliance process among stakeholders - front, middle and back office. Compliance is not the exclusive domain of the Compliance function which, as a second line of defense, is only one of the actors in these processes. Compliance risk management is everyone's business.
3. The industrialization of compliance processes through more and more elaborate information systems, for example regarding transactional supervision, tends to increase security and speed. The challenge for financial institutions is to develop intelligent information systems with increasingly complex settings. The aim is to generate better, not more, alerts.

Stricter regulatory requirements are causing compliance costs to rise significantly. Might this put more pressure on employees to take risks that could enhance profits but expose the banks?
The alleged loss of efficiency is a short-term view. Good compliance risk management allows an organization's value to be maintained over the long term. Today, the compliance risk is no longer theoretical since, in many institutions, it takes the form of increasingly high and numerous penalties. Investment in compliance helps preserve the long-term value of an establishment and can therefore be considered "profitable".

At the same time, many institutions are raising sales and control teams' awareness of risks that employees may incur, including sometimes at a personal level.

Potential conflict between the 'Front' and Compliance functions appears to be a caricature. There is a common objective to protect the bank and its reputation, even if the two functions may have occasional disagreements.

Banks faces commercial pressure to meet clients' funding needs in areas such as trade finance. These needs are often urgent and involve substantial amounts. How can the risks of exposure to penalties and fraud be mitigated while still meeting clients' needs?
As a competitive environment is riskier, it is essential to understand the client well. Not only the client but also the related counterparties and, more generally, the client's transactional profile. In this sense, the KYC process is a continuous exercise. This is an advantage of having long-term business relationships. A holistic approach to all of a client's transactions allows the banks to better understand the client, his counterparties, his risk appetite and his real level of sensitivity.

Monitoring and analyzing transactional alerts is a critical bank process, in particular due to the risk of violating embargos or AML rules. How do banks address this in an ever more competitive and restrictive environment?
In addition to the expertise of the business and control teams, one of the solutions is to use key information systems to avoid trade-offs between profitability and security. Ex-post transaction detection tools, which enable an understanding of a client's transactional profile, are increasingly sophisticated. How can supervisory systems be more elaborate while generating more relevant alerts? This necessarily involves investments in tools. In order to reconcile efficiency and safety, more and more financial institutions are working in collaboration with specialized fintechs.

> «Managing the unexpected is at the heart of Compliance. It's sort of its daily business.»

How does the bank ensure that it does not break sanctions rules, yet maintains funding activity with a country that represents a substantial part of its activity?
Sector-related sanctions aim to target and sanction key sectors of an economy. Sanction programs can be complex, so they require real expertise to determine what is strictly authorized from a regulatory point of view, and what is prohibited.

The response of the bank and other organizations is primarily to develop the Compliance Officers' expertise and build specialized competences according to geographic regions and sanction programs.

Sales teams must also be made aware of and trained in this issue by the Compliance function. Knowledge of international financial sanctions must now be part of the essential toolkit of control teams, certainly, but also of commercial teams.

Also, sales teams' annual evaluations are no longer based solely on commercial objectives, but also on risk control objectives, in particular compliance risk.

How can banks efficiently manage the extraordinary workload that arises during a crisis situation such as the Panama Papers?
Managing the unexpected is at the heart of Compliance. It's sort of its daily business.

The fundamental challenge for institutions is precisely to prevent crisis situations. It is essential that they act upstream of issues, for example by relying on rigorous selection and review processes and in-depth due diligence - knowledge of ultimate beneficial owners or UBOs, tax compliance, transparency of the origin of funds, etc.

In a crisis situation, it is essential to react quickly by dealing with the information coming, for example, from the press which are sometimes contradictory and systematically need to be confirmed and made reliable. It is necessary to process, analyze, extract and ensure the reliability of a large amount of data over a short time span. All while communicating fluid and transparent information to management.

The first step thus consists of defining rapidly a clear governance system, e.g. by setting up a dedicated task force or crisis unit in which management and all the concerned services must be involved and committed.

What compliance challenges arise from new, less regulated technologies such as blockchain and cryptocurrencies?
Blockchain can raise questions concerning energy, economic and environmental sustainability, but also legal and value chain governance. Cryptocurrencies tend to raise issues about opacity and lack of regulation, which, from the point of view of compliance, generates risk. Cryptocurrencies also raise ethical and reputational questions, to which answers are not yet satisfactory from many financial institutions which mostly follow a prudent approach. These and resulting changes represent a real challenge for the banking industry as a whole, not only for the Compliance function.

What major compliance changes has technology produced? Do you think artificial intelligence will replace human beings in the future or will human intervention remain necessary?
Compliance risk management relies increasingly on information systems, which are an increasingly essential complement to human resources. In terms of security and efficiency, technology is a major source of opportunity for compliance risk management. However, it is also a challenge, as banks rely on increasingly sophisticated tools that the Compliance function must master. The profile of compliance officers must evolve: they must no longer be only regulation, control and risk experts but must also master information systems. Some banks now incorporate IT specialists in their compliance teams.

If technology generates alerts, human beings make them talk. People therefore remain and will remain indispensable, but they will have to develop and extend their expertise in new tools as our environment continues to evolve.

04

The human factor: filling the gaps with specialist knowledge

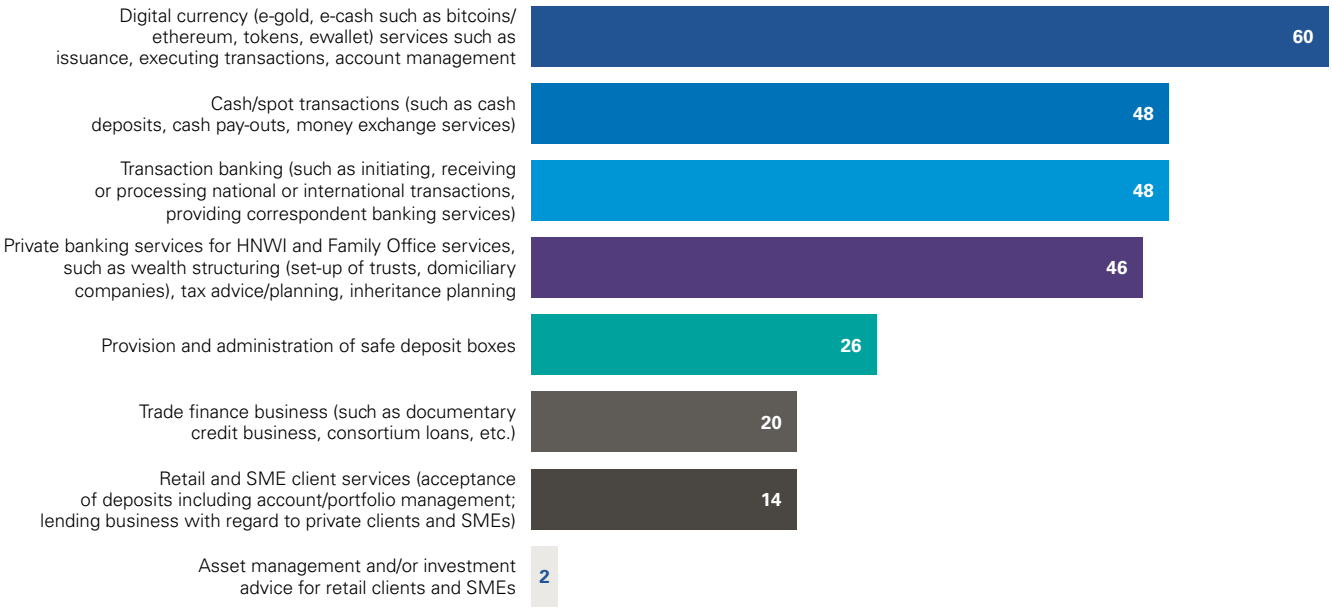
The detection and prevention of financial crime would be significantly improved through greater investments in specialist support to raise the quality of data and analysis.

Risks and uncertainty are greater in areas of limited knowledge or poor data

Ignorance of the facts and figures creates uncertainty and dangers. Combined with low quality data, the risks to the bank increase. This can be mitigated by specialists and tools, particularly with regard to threats arising from new markets or technologies.

- 60% of banks see the greatest risks being in digital currencies, 48% transaction banking, and 48% cash or spot transactions

Which products/services do you think are exposed to an increased financial crime risk? (in percent)



While banks already make significant investments in their people, more is needed

- Human resources are the primary area of investment to overcome financial crime, at almost 40% of banks. This is followed closely by investment in infrastructure and IT, at 38%
- Yet, 23% of respondents say more investment in staff would be most helpful. An equal number would like to see a larger budget for IT infrastructure and innovative solutions

Banks do not recognize enough the role specialists play in combating financial crime

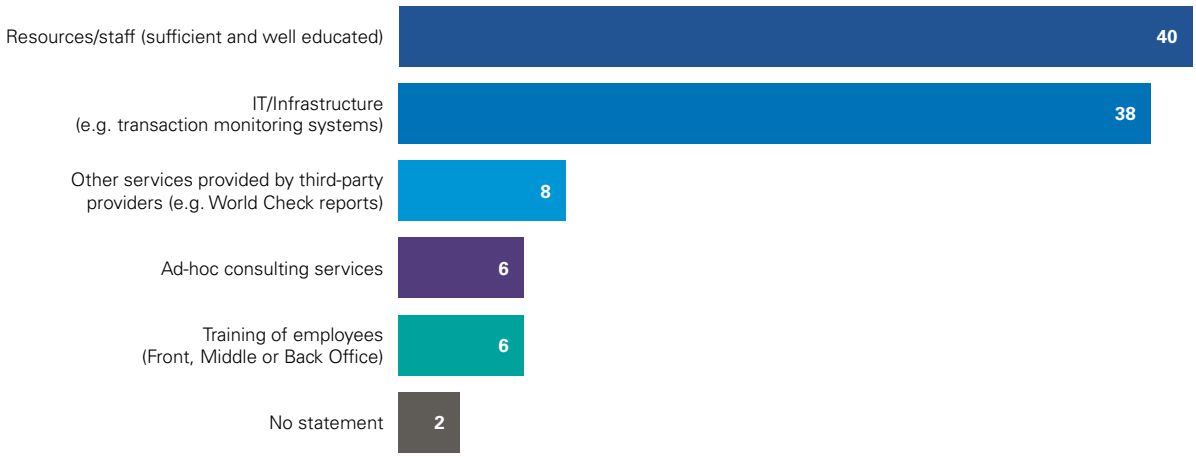
In-house specialists and external experts are key to banks' efforts against financial crime. But banks tend to believe a generalist Compliance function is enough.

Specialist teams at the bank help to detect financial crime before third parties do so

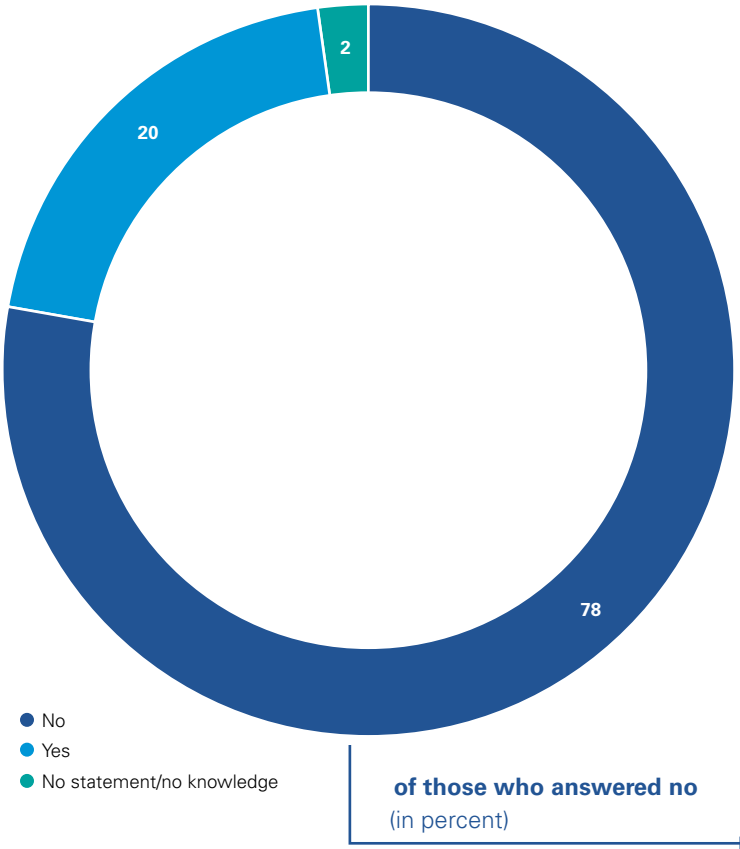
Third parties too often identify financial crime before the bank is even aware there is an issue. Specialist teams at a bank can be instrumental in rectifying this situation. By detecting crime earlier, there is less chance of the bank being caught by surprise by media reports or other sources, allowing a more proactive treatment and potentially lower reputational or financial harm

- In-house specialists:
  - More than 60% of respondents indicated that the responsibility regarding financial crimes lies with Compliance/Risk
  - Only 20% of banks have, or are currently setting up, a specialist team that investigates and deals specifically with financial crime
  - Of these 20%, cases of financial crime were discovered internally (e.g. by employees) in two-thirds of cases
- External specialists:
  - Involvement of external specialists is not (yet) a priority topic in banks' efforts to reduce financial crime, though it should be
  - Only 6% of banks purchase consulting services on an ad hoc basis
  - 8% of respondents would like additional, external support to complement their internal resources

Where is your bank currently investing primarily to overcome financial crimes? (in percent)



Did your bank build a new/specialized team investigating/handling specifically financial crimes? (in percent)



of those who answered no (in percent)

Agenda for action

- When investing in additional resource, ensure the resource is adequate and specialized
- Diligent and highly educated first line of defense that understands the banks risk appetite, tuned to speak up if they detect anything suspicious
- A specialist crisis team enables agile structures to provide swift responses to unexpected events
- Consider engaging external specialists to complement internal capabilities where the building of sufficient internal resources is too expensive or impractical

From reaction to managed action: turning the tide with digital forensic readiness

Much-needed improvements and flexibility can be created by expanding digital platforms to cover systems and information channels that are accessible to both internal and external parties. But doing so also increases the surface area for digital risk. What approaches can help banks deal with this new exposure in a digitalizing environment?

Digital forensic readiness ('DFR') is a response plan that helps organizations control the potential impacts created by a digital economy. These include digital incidents such as a cyber attack, human error or sabotage, or other events such as a regulatory inquiry or internal investigation that relies on the identification, preservation and analysis of digital evidence. Integrating DFR into the overall risk management approach should be a natural step for any organization. Systems, applications and platforms at risk or that store digital information should be looked at through a forensic lens, not only from an operational or business continuity perspective.

DFR encompasses various elements including strategy, governance, people, process and technology. All require buy-in from key stakeholders within the bank. These include the IT function as a key participant, for whom the primary challenge is to form a clear picture of which digital information is stored where, what is available, and what could potentially be in scope for an inquiry or investigation. And then ensuring its quality, integrity, completeness, traceability and defensibility.

Limiting any damage

It is no longer a matter of if a digital incident will occur, but when. DFR highlights the need to transition from a reactive model that lacks clear process to an actively managed model that allows a bank to be in control and limit the damage caused by a digital incident. A forensic-ready organization is one that:

- can issue a timely and effective response
- has established partnerships with external specialists and stakeholders that can be involved as required
- periodically rehearses, evaluates and updates the response plan.

A bank's DFR maturity will reflect its position when a digital incident or event requiring a digital investigation occurs. For instance, internal and external stakeholders are defined and can be notified promptly - in Legal, Risk, IT and other relevant departments, as well as regulatory authorities and potentially law enforcement. Roles, responsibilities, escalation guidelines and communication channels are established. The incident response team or task force is prepared to rapidly safeguard all potentially relevant data in accordance with planned procedures. The stage is set for a comprehensive assessment, the investigative methodology is defined and appropriate countermeasures can be employed quickly.

Containing the costs

An immature DFR position, or a reactive, improvised approach, may cause the rapid loss of control over factors that cause expense. This is especially the case when a lack of structure or plan impedes the bank's ability to lead or cooperate with investigations or other forms of review, for instance large volumes of data are involved. In addition, a growing number of organizations are being sanctioned for their inability to retain, identify preserve, and produce relevant information for a regulatory inquiry or litigation. DFR helps to contain all these manageable factors.

Towards continuous improvement

The DFR should include regular vetting of shortlisted, preferred service providers, an up-to-date vendor service map, out-sourcing and on-boarding process in place, with corresponding Master Service Agreements, and retainers where appropriate.

The experience gained across all relevant areas is valuable intelligence that will help to re-evaluate and adjust the risk management approach and assessment of the digital threat landscape. Periodically rehearsing, evaluating and updating the response plan, or playbook, is essential to DFR. For this, the tracking of relevant metrics and KPIs is important to increase efficiency and cost control. Learning from your own organization and from peers can help the DFR to evolve and improve.

Given the nature of the underlying risks and the likelihood of such risks becoming incidents or events, aiming for DFR maturity and an in-house response capacity is not only sensible from a business perspective. A business-centered, mature DFR approach will have the right interface with external, established partners for rapid deployment or involvement when it is most needed.

Towards greater regulatory compliance: the need for enhanced client due diligence

As the world's largest center for cross-border wealth management for private clients, Switzerland's financial institutions manage one-quarter of global cross-border assets. With the country's financial system exposed to a high risk of asset-based money laundering, what more should Swiss banks do to combat crime originating in Switzerland or abroad?

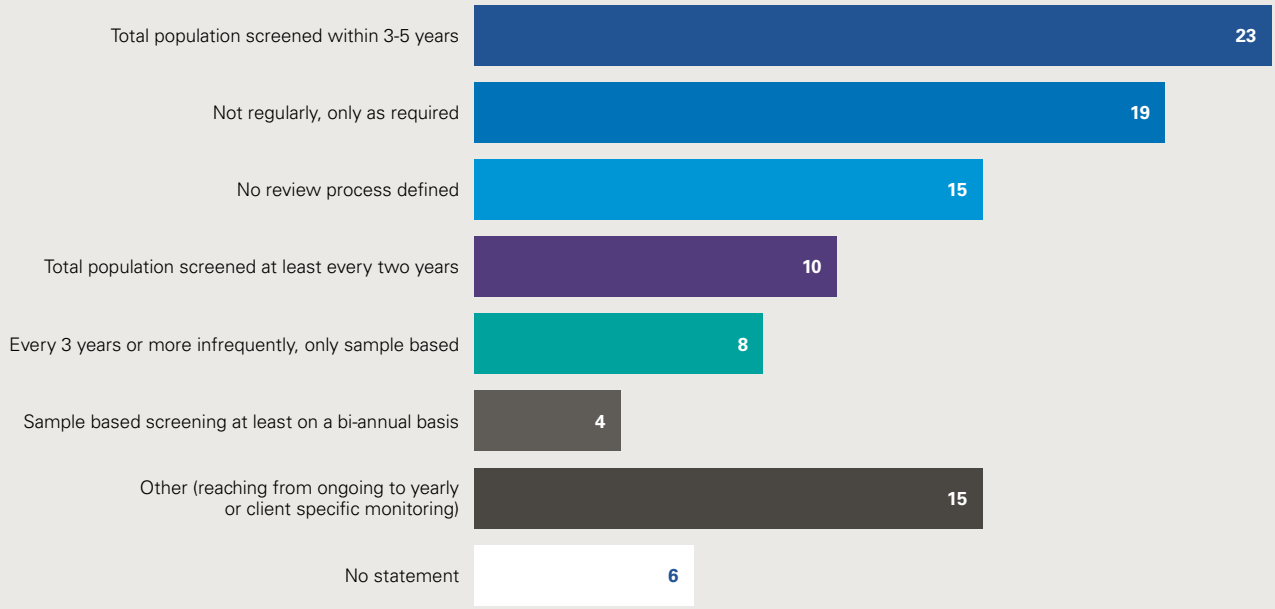
Hundreds of billions of Swiss francs of criminal origin are laundered through the world's financial system. Data leaks such as the 'Paradise Papers' pick up where the 'Panama Papers' left off, indicating the scale of the problem as money flows through multiple jurisdictions, clouding the audit trail as it goes.

Banks have a duty to gather information about their clients prior to and during the relationship, taking particular account of money laundering and terrorism financing issues. But according to the Financial Action Task Force (FATF) report on anti-money laundering and counter-terrorist financing measures, Swiss institutions do not perform adequate or satisfactory client due diligence. This is particularly the case in longstanding client relationships classified by the bank as low or medium risk.

New regulation necessitates more regular reviews

Based on the FATF report, the Swiss Financial Market Supervisory Authority (FINMA) as well as the Federal Council have launched a consultation on the revised draft of the FINMA Anti-Money Laundering Ordinance and of the Anti Money Laundering Act respectively.

The FATF criticized Switzerland for focusing on high-risk relationships and neglecting a reliable monitoring of long-term and low/medium risk relationships. In your bank, how often do you monitor long-term (older than five years) relationships classified as low/medium risk? (in percent)



New mandatory requirements would include regular updates of client information and the verification of information related to the beneficial ownership for the entire client population (low as well as high-risk clients). Any amendments would most likely not enter into force before 2019.

The results of our survey show that considerable improvement in the monitoring of clients is needed. 15% of respondent banks have no defined review process, 19% do not undertake regular reviews of the relationship, and 8% undertake sample based reviews but only every three years. Only 33% of the interviewed review the whole client population within two to five years.

Revisiting client information

To ensure the appropriate classification of clients, reviews should be carried out on a regular basis to answer questions such as:

- What enhanced due diligence has been carried out, and when?
- Have the necessary KYC reviews been conducted since the onboarding, reflecting the fact that policies may have changed in the meantime?
- What is the current classification of the client and is this in line with anti-money laundering policies?
- Is all necessary documentation such as corroborating documents, adverse media checks etc. available?
- Did the identified sources of funds comply with current requirements?

An ever greater need for due diligence

Conducting an accurate due diligence and onboarding is key. Financial institutions may perform desktop due diligence on low-risk clients, with most using World-Check. For potentially high-risk clients a full due diligence is needed - i.e. a detailed analysis of the customer relationship. This may become the case for low-risk clients too.

Of course, globalization and cross-border relationships raise obstacles in the form of language barriers and different regulatory environments and jurisdictions. This makes the collection and processing of information more difficult and time consuming. Especially where there might be a lack of publicly available or accessible information about a customer, or where the customer is domiciled in a country that is out of the bank's reach. Without an established network, the chances of obtaining the necessary information in due time are low. Yet, the growing need to obtain crucial information exposes the organization to numerous risks. Meaning that concerted effort and specialized solutions are required to proactively handle the delicate task of obtaining insights on new and existing clients.

Going the extra mile to obtain meaningful and reliable insight into customers' backgrounds will help assess, mitigate and potentially eliminate financial, reputational, legal or regulatory risks. And crucially, help banks make well-informed business decisions.

Astrus due diligence reports help you gain insights into individuals and entities

Astrus is a digital solution developed by KPMG to help you get information on your potential customers or other third parties. This includes vital data on their backgrounds, adverse press and any sanctions imposed.

Our concise and comprehensive reports highlight key issues and provide clear risk indicators. Astrus has access to World-Check, but this is only one of many sources we use in our extensive worldwide network of public and non-public information sources. In fact, our forensic-minded people are fluent in 88 languages and have gathered information from more than 40,000 online data sources around the world. We also utilize the world's largest and most comprehensive third-party data aggregators to analyze facts.

You will receive a screening report containing a risk summary, background details, adverse press and media content, as well as information about PEPs, sanctions and other high risks. You can also receive an enhanced due diligence report that consider ownership structures, litigation, career development, corporate interests and much more. In addition to any specific requests you might have. Our reports are prepared within two to six working days.

05

Critical components for robust compliance: strong culture, tone at the top and an effective sanction system

A strong compliance culture and appropriate tone from the top is important, but is not by itself sufficient to prevent financial crime. Actually enforcing sanctions against employees who breach compliance policies is likewise essential.

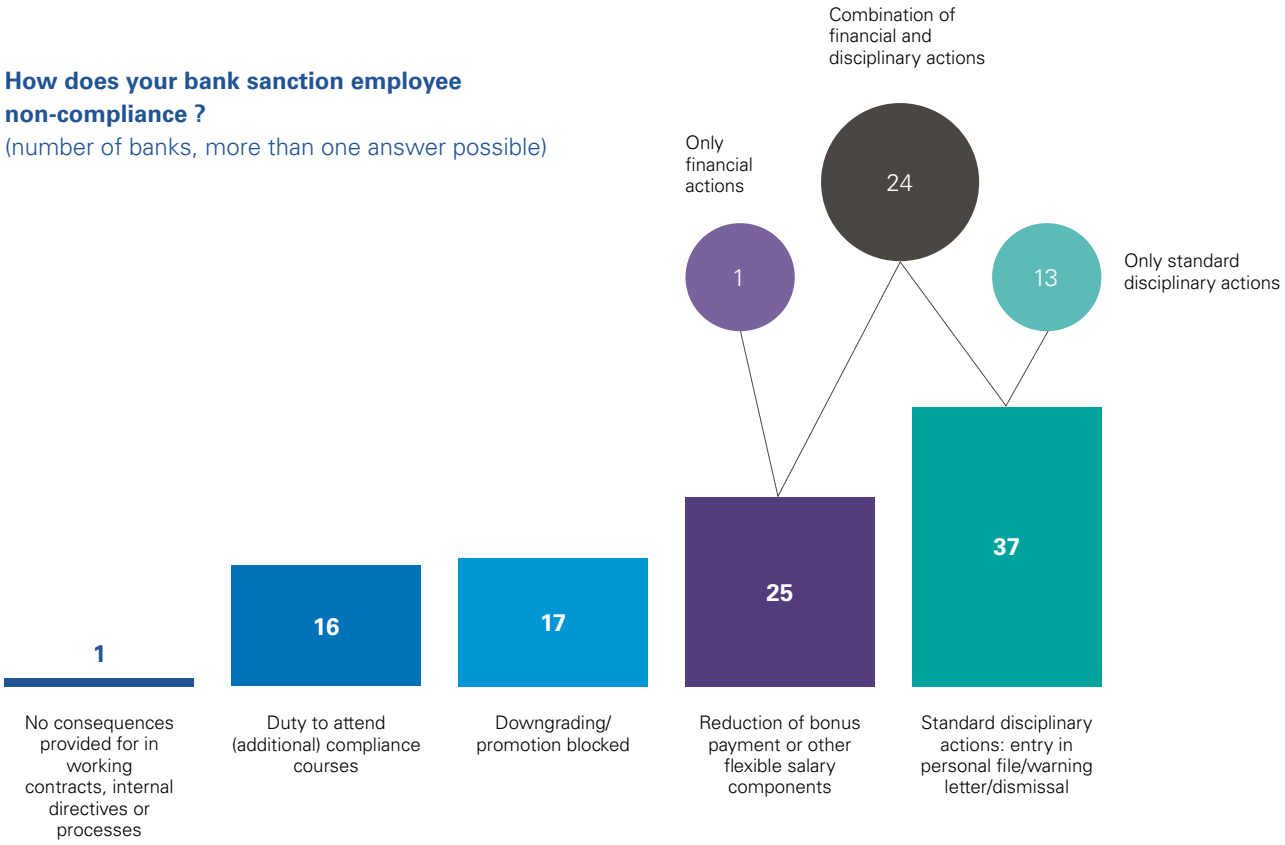
The tone at the top is essential for a good compliance culture. However, a combination of several factors makes the difference

Senior management's tone is essential to consistent and efficient compliance, but compliance can be most effective when this is combined with an embedded compliance culture and effective sanctions for misconduct.

- 88% of banks agree that the tone at the top is essential to consistent and efficient compliance
- 37 of the 50 banks consider disciplinary action to be the most effective at encouraging compliant employee conduct. Of these, 24 hold believe a combination of disciplinary and financial sanctions that is most effective

How does your bank sanction employee non-compliance ?

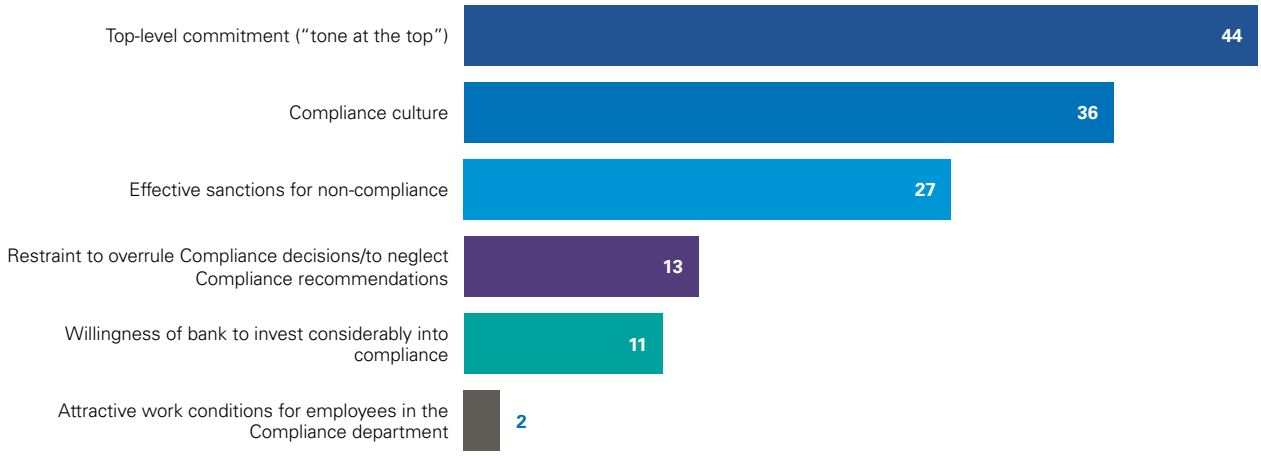
(number of banks, more than one answer possible)



A good compliance culture is one where employees are incentivized to behave appropriately, and sanctioned where their activity breaches the bank's compliance code

- Despite a good compliance culture, banks continue to be affected by financial crime. Sanctions for non-compliance are needed alongside incentives for exemplary behavior
- Banks that see a good compliance culture as more important than sanctions have been more often subject to a financial crime in the past three years
  - One in five banks who consider a compliance culture to be important have not been subject to a financial crime in the past three years, and 14% have never been
  - By contrast, two in five banks who believe sanctions for non-compliance are critical have not been involved in a financial crime in the past three years, and 15% never

What kind of corporate attitude is essential for an overall consistent and efficient compliance? (number of banks, more than one answer possible)



It appears that the tone at the top is not lived throughout the organization

- Respondents ranked the independence of the Compliance function to be the most important factor in an efficient and successful function. Yet, the option of contributing on an ad hoc basis to board meetings was ranked the least important
- Overall, our findings suggest that while the tone at the top may be correct and appropriate, it does not cascade throughout the banks and is therefore not 'lived and breathed'

Required governance for an efficient and successful Compliance

Agenda for action

- Keep the Board of Directors timely and transparently informed of compliance matters
- Ensure the Board of Directors or Executive Board have sufficient information to enable them to provide appropriate oversight
- The Board of Directors need to develop and implement a comprehensive risk appetite framework according to the bank's business model
  Defining your risk appetite: key questions the Board of Directors should ask
  - How strict should our client acceptance procedures be?
  - What does it take for us to exit a certain client or client segment?
  - How quickly can and should we file a notification?
  - How do we sanction employees for non-compliance?
  - How do we ensure sanctions are enforced?
- Give Compliance the possibility of escalating matters to the Board of Directors on an ad hoc basis to give it greater leverage and allow it to demonstrate independence in encouraging the bank and board to operate in accordance with the defined risk appetite
- Implement consistent guidelines and a manageable number of AML guidelines to encourage employees to adhere to compliant processes
- Be in a position to impose disciplinary and financial sanctions on employees. The process for this must be independent and impartial if it to be effective and accepted by employees

Three key elements of an effective compliance system

Financial institutions are too often perceived as having poor business cultures and suffer heavy criticism from a range of stakeholders regarding their business conduct. Partly contributing to this is the fact that financial institutions worldwide have been fined with billions of Dollars since the financial crisis. As financial institutions face an urgent need to maintain or rebuild trust and confidence, what are the three essential elements of an effective compliance culture?

Take preventative measures

One of the most important elements is the tone at the top. Senior management must lead by example and emphasize the importance of compliance for business success. One such example comes from Warren Buffett, who addressed a letter to his management, saying: "We can afford to lose money – even a lot of money. But we can't afford to lose reputation – even a shred of reputation."[1]

Senior representation for compliance is also important. The Head of Compliance should be a member of the Executive Board. This allows him or her to discuss compliance topics in person and as an equal rather than relying on the submission of reports.

Good compliance is not restricted to an organization's leadership, of course. Continuous training and awareness building of employees is of huge importance. Together with follow ups such as tests to assess how effectively the compliance culture is being lived in the organization.

Put in place effective control systems

Empirical research shows that non-compliance is higher when employees believe their non-compliant behaviour will go undetected.[2]

Effective control mechanisms must therefore be in force, whether in the form of sampling or 100% controls. It remains very difficult to measure 'culture', however. This is why new techniques such as verbatim text analytics have been developed to measure data that would otherwise be almost impossible to analyze.

Sanctions for breaches of compliance

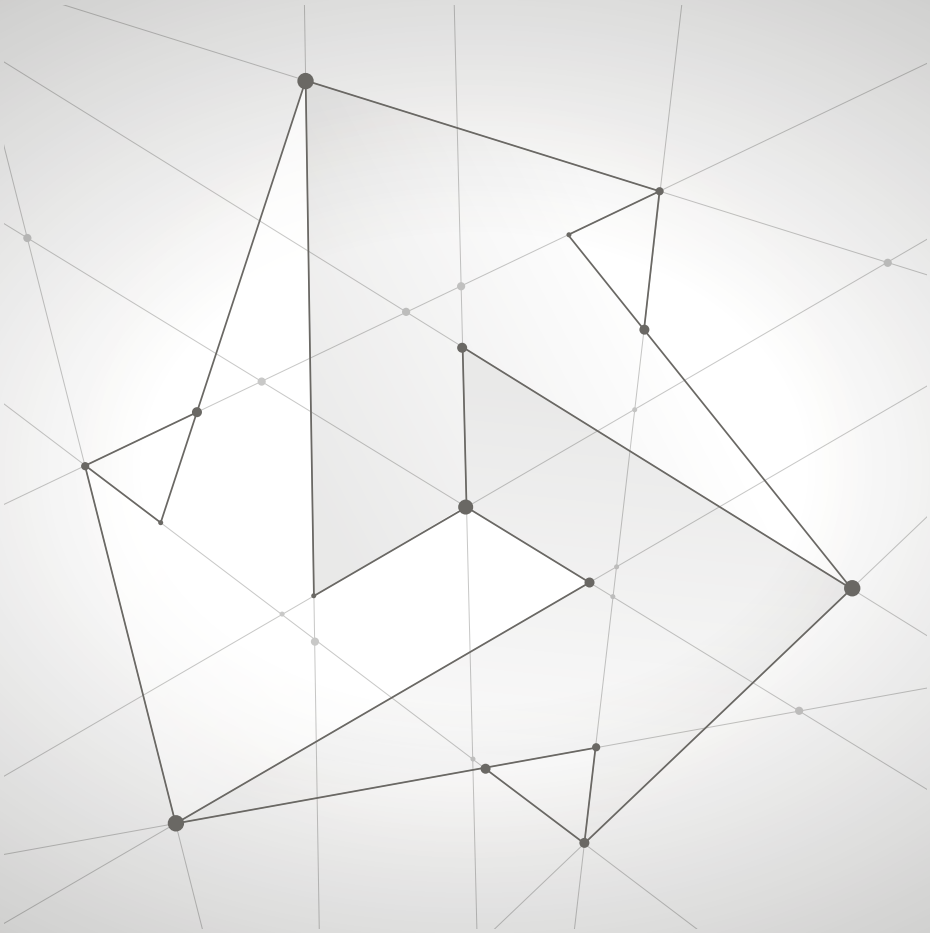
Non-compliant behaviour must have disciplinary consequences for the employee, supervisor or entire team, if a culture of 'results at any costs' is to be discouraged.

Ideally, a sanctions committee would be responsible for deciding the appropriate sanctions. Such a committee should comprise the Head of Business unit to provide the business perspective, the Head of Compliance and a member of the Board of Directors or Executive Board. The goal of sanctions should be to punish non-compliant behavior while avoiding the creation of an atmosphere of fear, as the latter could encourage employees to avoid reporting compliance breaches.

It is only by incorporating all three of these factors in their compliance set up that financial institutions will achieve a reliable, effective compliance culture. And maintain the trust that goes with it.

[1] Buffett Warren E., Memo to Berkshire Hathaway Managers from July 23, 2008, https://www2.bc.edu/robert-radin/Administration/Buffett%20Managers%20Letter%202008.pdf

[2] Schulz Martin/Muth Thomas, Erfolgsfaktor Compliance-Kultur, 270.



From the top: effective anti-corruption measures and the need for change

Gemma Aiolfi, Head of Compliance, Corporate Governance and Collective Action at the Basel Institute on Governance, discusses the challenges facing banks in combating financial crime, including the need for senior management to lead by example.

Gemma Aiolfi, Head of Compliance, Corporate Governance and Collective Action at the Basel Institute on Governance

KPMG *Recent years have seen some significant corruption investigations and prosecutions of companies, though we are fortunate in Switzerland to have a low rate of corruption. Is anti-bribery and corruption a topic for Swiss financial institutions?*

Aiolfi As the former, first global head of anti-corruption at UBS, I have to say yes, it is. Looking at the client risk first, Switzerland is home to many multinationals that operate around the globe. They may be operating in corrupt environments, so this may present risks for financial institutions, if for example money is transferred by the company through the Swiss financial system to pay a bribe abroad or even here. Then there is the risk of money laundering of the proceeds of corruption through transactions involving Swiss financial institutions. Secondly, Swiss banks operating internationally may themselves run risks through their employees when acquiring new business. For example, seeking government clients through intermediaries who may pay a bribe on behalf of the bank, or dealing with foreign public officials in ways that could be construed as corrupt. So when Swiss institutions pursue business abroad, they must ensure employees abide by Swiss criminal law. So yes, it is definitely a topic for Swiss financial institutions both from the client side and regarding their own staff seeking new - or retaining existing - business.

What challenges face Swiss financial institutions in terms of combating corruption?

It's interesting to see that the Wolfsberg group has reissued its guidance on combating corruption: In its latest version published last year it focuses almost exclusively on what a financial institution's internal program should look like. When you look at the sequence of their guideline updates over the years this wasn't always the case. The first paper in 2004 started off as a statement that corruption is a problem, and our biggest problem is probably with our customers. As time went on, it was reissued to address risks raised by employees as well as the customer risk. The latest incarnation of the guidance acknowledges that customer risk is addressed by anti-money laundering measures and rather covers prevention relating to risks that employees may present. The guidance sets out what a financial institution's anti-corruption program should address. It's interesting to see how the focus has changed as they became more aware of their own risks as distinct to those of the client. Many corruption cases involve the use of intermediaries – banks may be misused to enable money to be paid as a bribe or to pass through to an intermediary. To identify this among the mass of legitimate transactions remains a challenge. Transaction monitoring is key but it needs to be combined with a thorough understanding of the business model that the company operates under. If a company's business model is to win business through bribery and they set up complex offshore structures without reasonable explanations, use accounts that are off balance sheets, for example, then transfer money into those vehicles in preparation of paying bribes, it would be hoped that the bank has systems in place to raise alerts that enable questions to be asked of the client.

What in your view are the essential components of an anti-corruption compliance program?

There is lots of guidance out there, from the OECD, UN, ISO standards as well as from the US, UK and France and so on, that aren't specifically targeted at the financial industry. But the latest version of Wolfsberg's guidance focuses on that question: It starts off by recognizing that no one size fits all, and that the risk-based approach matters. On that basis, anti-corruption risk mapping and risk assessments specifically relating to corruption are important. The governance of the program is also very important, having clearly defined responsibilities as to who should run it, who should devise it and so on.

Part of the risk mapping includes interactions with public officials, understanding with whom you're dealing as a potential customer. This is no different to any other industry in terms of gifts and entertainment, sponsorship, donations, political donations. It should be about how does the bank actually operate in practice in any given market. Having a whistle blowing or advice hotline is key in all anti-corruption compliance programs. And the usual elements of policies and procedures, training, tone from the top and good governance, are all important components.

You mention the tone at the top, which our survey shows is one of the most important elements. The Basel Committee Guideline "Compliance & the Compliance Function in Banks" from 2005 states that "…a bank's compliance policy will not be effective unless the Board of Directors promotes the value of honesty and integrity throughout the organization." Why do you think the board plays such an important role when it comes to a good compliance culture?

The Board of Directors is responsible for approving and agreeing the risk appetite, which sets the parameters for behavior in the company, how you get new business and at what price. Everything flows from the top, therefore. Most people want to do the right thing and to work for an organization that conducts itself with integrity. It's important that this is not only in regard to legal and regulatory obligations so the board sets the ethical tone as well. Plus the board has to exercise oversight, ensuring the company's long-term interests, leaving their personal interests on one side and serving the stakeholders, acting in the best interests of the organization overall. The board and senior management set the tone from the top, they are the embodiment of the corporate culture. But tone is not enough, it's got to be followed up by action, including from the top.

Survey participants noted that direct access for Compliance to the board is not very important. Rather, Compliance's independence is of greatest importance. What is your view on this?

Independence is crucial to ensure that compliance can function effectively to prevent, detect and respond to risks and breaches of policies and the Code of Conduct. In my view, independence is closely linked to direct access to the board. I would recommend that a board invites the Compliance function to contribute on a regular basis to its deliberations, and Compliance informs, advises and can candidly report on risks. The board for its part must really engage with compliance, raise questions and go beyond pro-forma receiving of reports, so the tone from the top can be actively formulated. If Compliance reports are regarded as pro forma, it could suggest that the board is not being challenged, or that the board is not really engaged. Compliance having direct access to the board is part of its independence; it gives the Compliance function authority and status within the organization. Financial institutions are hierarchical, and direct access to the board confers status. What you also need is people on the board who understand what compliance is about, and don't see it as a block to the business, but who actually appreciate it. Compliance should be seen as supporting the business, acting independently and advising like a critical friend.

What would you require the board to do when it comes to combating financial crime?

There is a duty to set the risk appetite based on an active understanding of the nature of financial crimes that can confront the organization. There is no one size fits all for these things.

«Swiss banks operating internationally may themselves run risks through their employees when acquiring new business.»

Part of the risk-based approach is to understand different aspects of what the financial institution faces. There is an ongoing obligation for the board of directors to understand the risks. Changes in the business, or opportunities to gain new clients, present all sorts of different risks and ways to present financial crime risks. The board also has to be self-critical as to its skill set - are they actually able to execute their responsibilities properly? If not, how do they equip themselves to do so? Do they have the right composition? Relevant experience and knowledge? If not, take action to do something about it.

What instruments and pragmatic solutions are key to lower management being compliant?

Support from higher management and seeing senior management set an example. But also important are adequate channels to get help and advice and knowing the policies and procedures and a culture of asking questions when you are not sure. The pragmatic solution is an open door, where people sit together so that compliance isn't something remote, rather it is accessible and present. There are all sorts of IT tools, but at the end of the day it's an open culture and being able to say to your boss, "Something is not right here" or "I didn't feel comfortable with this." Scandals and the financial crisis highlighted the role of risky business targets and methods for acquiring business, and a bonus culture that rewards risk-taking on a level that is inadvisable. Incredibly important is a statement by senior management to reinforce the positive impacts compliance has on the organization, for instance in ensuring that we say yes only to good or clean business. To have that in your code of conduct or repeated often is very important. It is also a good idea to rotate people through compliance as part of their talent development. It would help to change compliance culture throughout the organization and I think there are probably quite a few investment bankers who would benefit from this.

06

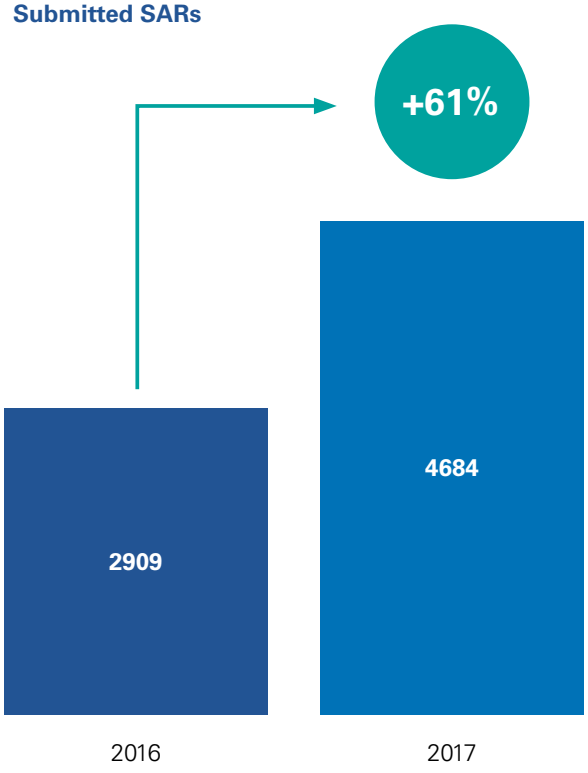
MROS notifications must be based on quality

It is the responsibility of banks to ensure that MROS notifications are appropriate and necessary, and that the motivation behind the notification is correct. By swamping the MROS with low quality notifications, banks could be limiting its ability to effectively filter and forward cases to law enforcement agencies. Ironically, therefore, the increase in not appropriate notifications ultimately produces a riskier environment.

The number of MROS notifications increased dramatically in 2017

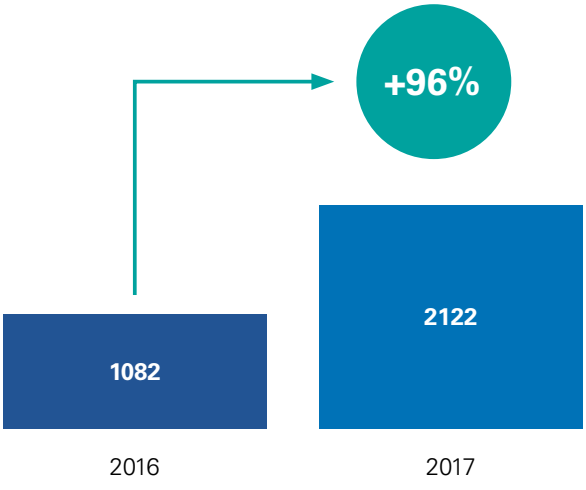
- A 61% increase in the number of MROS notifications, and a 96% increase in mandatory suspicious activity reports, last year suggests that notifications are being submitted without due consideration of their appropriateness or quality
- Authorities are struggling to process the volume of notifications, meaning that action on potentially successful prosecutions could be delayed or not take place at all

Submitted SARs



Source: MROS Annual Report 2017, p. 9

SARs submitted under art. 9 AMLA



Source: MROS Annual Report 2017, p. 10

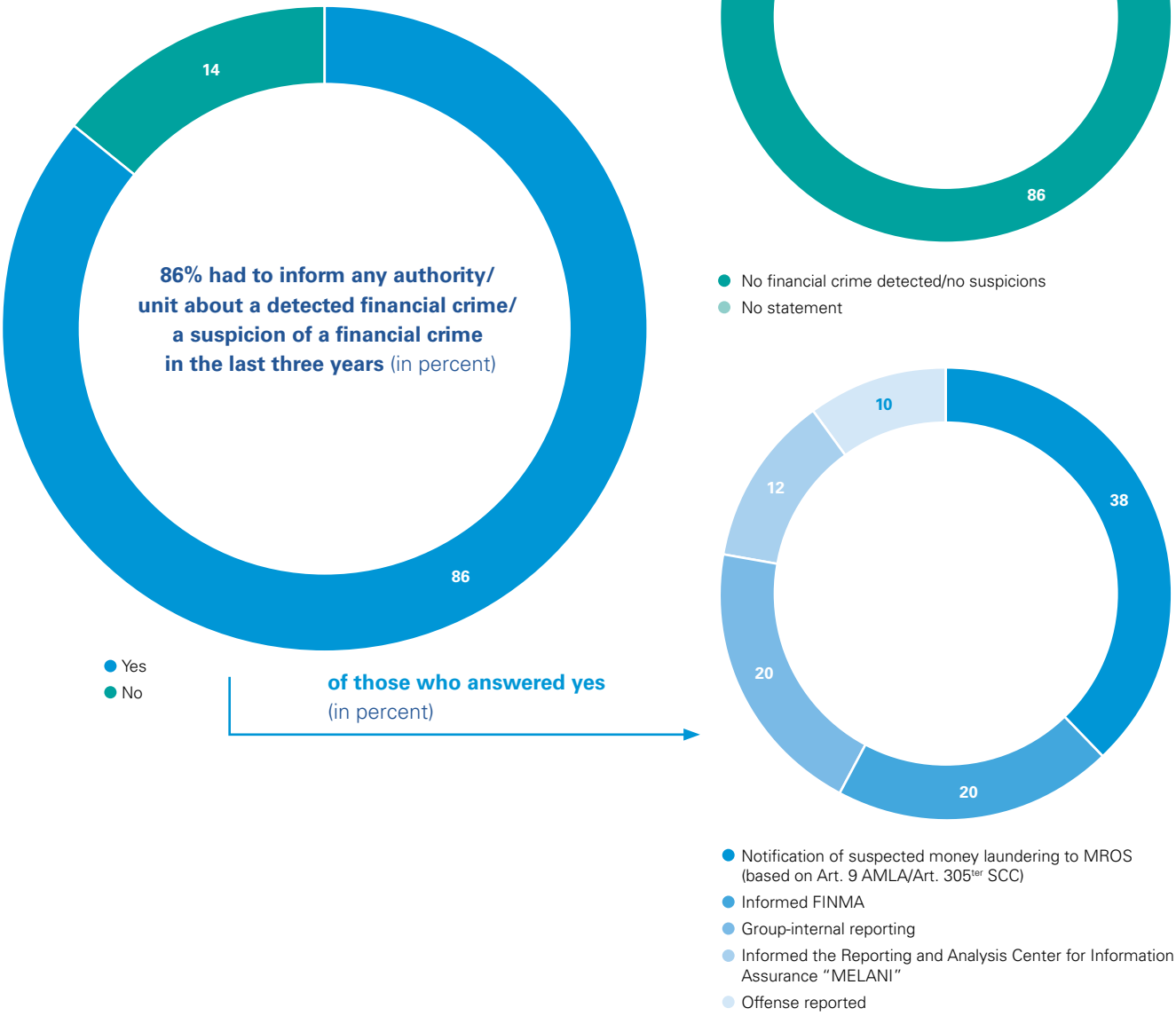
Many notifications may be submitted for the wrong reasons

The increase in the number of notifications may be due to a combination of factors: fear of the regulator, fear of reputational damage, uncertainty about how to apply the relevant legislation, a better understanding of the client, and enhancement of data quality still being insufficient.

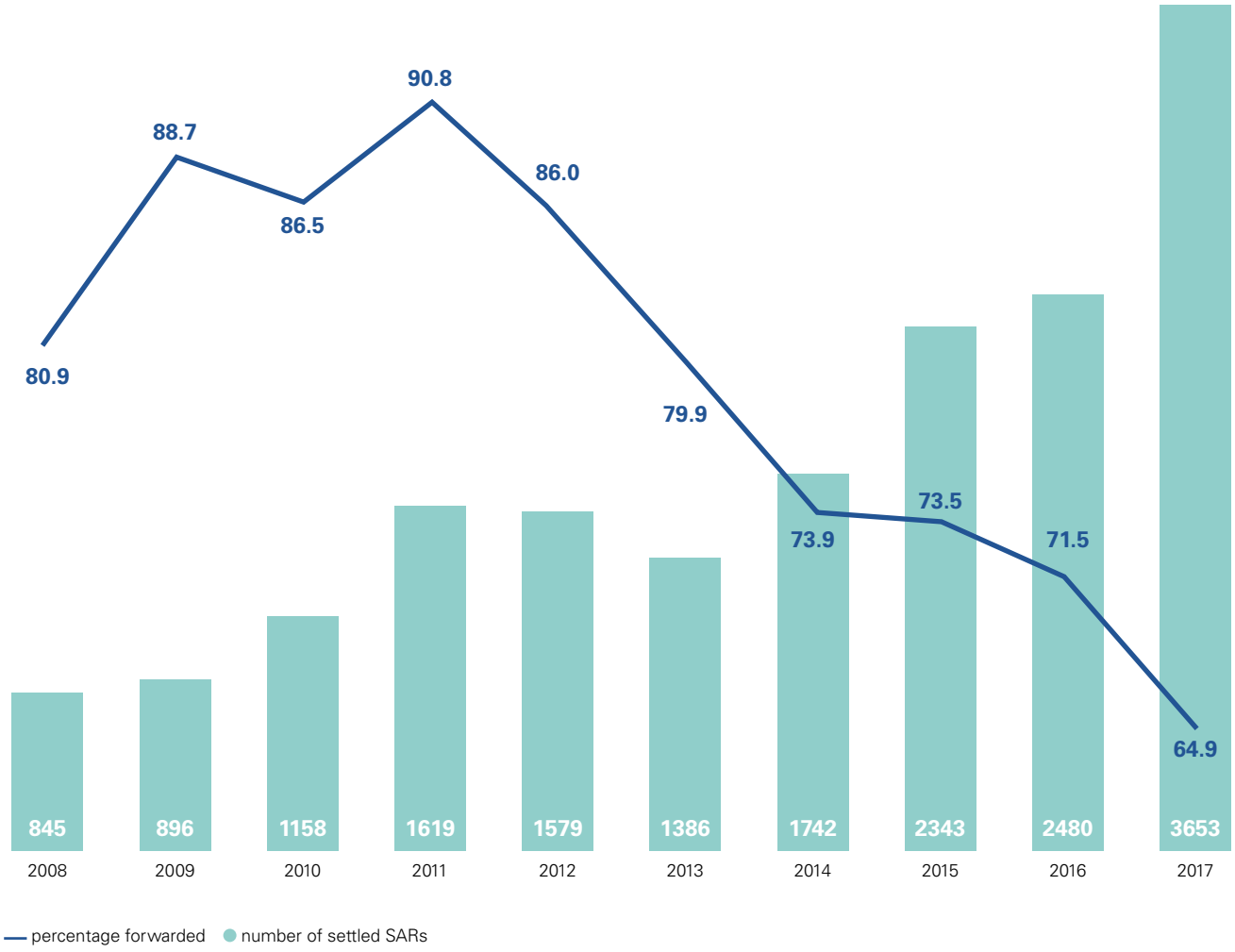
- 36 banks said the biggest challenge they face in combating financial crime is the increased expectations of regulators

The quality of MROS notifications has not improved compared to 2016

- The number of cases reported by MROS to law enforcement authorities has fallen steadily since 2011, from 90.8% to 64.9% in 2017



Total number of SARs settled by year and percentage forwarded 2008–2017



Source: MROS Annual Report 2017, p. 15

Agenda for action

- Use extensive client reviews to improve processes and systems, purge the client base of undesirable clients, improve data quality, and enhance the management and identification of risks and behaviors based on the organization's risk appetite
- Increase awareness and acceptance of front-to-back ownership at the first line of defense, and to improve cooperation between the first and second lines of defense
- Exchange knowledge with other financial institutions and the relevant authorities, e.g. through a database such as the Reporting and Analysis Centre for Information Assurance (MELANI)
- Share appropriate knowledge more broadly with the private sector to enhance collaborative efforts in the identification, assessment and mitigation of risks

Using social media intelligence to battle criminal financing

Social media is an important fundraising tool for criminals, particularly for terrorism or under the pretence of being a charity. Platforms can be used in the same way as any other group pursuing a cause: identify target group, convey urgency with propaganda and conclude with a call to action to contribute money. Too often, donors believe they are contributing to a legitimate charity. How can banks better protect themselves, donors and society at large from such activities?

Banks are able to screen and blacklist 'charities' that are known for illegal activities. But by the time the blacklist is produced, it is already out of date. In looking at how to apply the most current forms of information, one might be drawn to social media. But the considerations surrounding banks' use of social media data are extensive and complex. There are clear technical, legal, financial and ethical constraints regarding conducting social media intelligence.

Balancing the rights and wrongs of data use

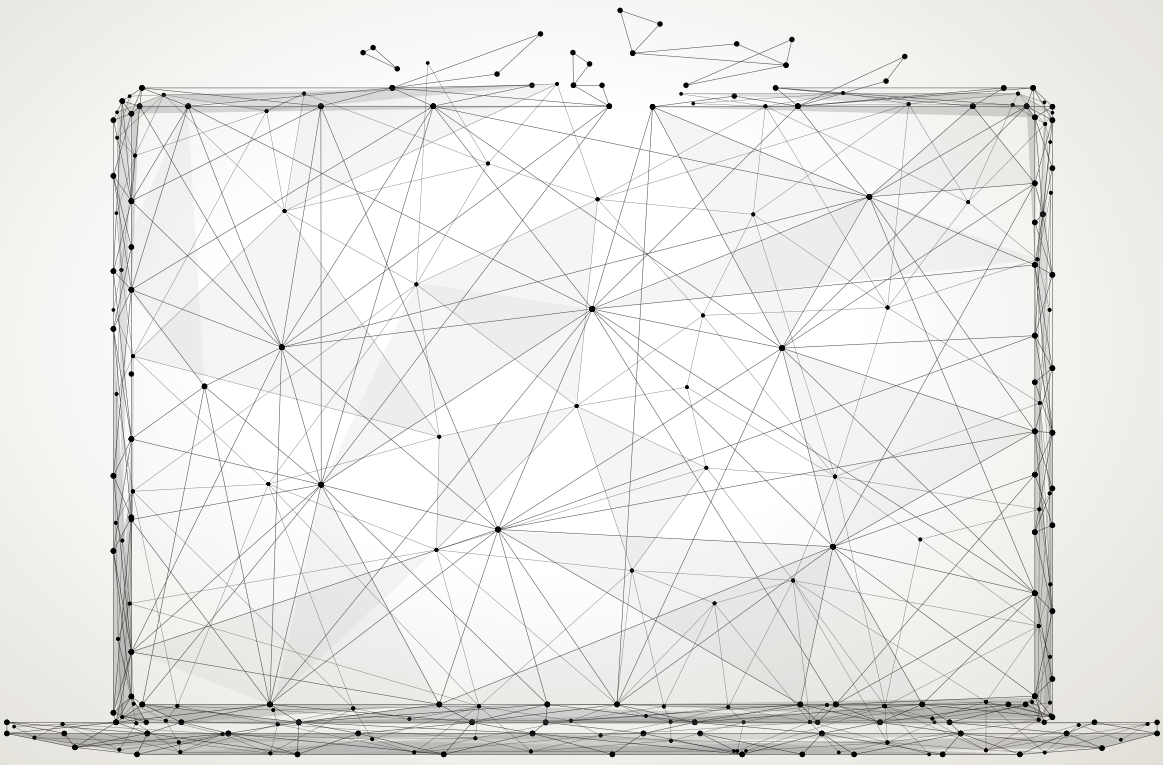
Certainly, banks have never had such extensive surveillance possibilities. Indeed, one could argue that they should never have. Nonetheless, financial institutions need to ask themselves how they can use social media intelligence and big data to enhance compliance. One possibility is to use existing social media data acquired legally and appropriately from specialist service providers in the field of data mining, in combination with meta data to screen it for indicators of criminal financing. By doing so, banks would be able to detect suspicious behavior more rapidly and effectively. Another possibility is that the Swiss authorities conduct social media intelligence themselves and establish a way to share this information with the financial sector. Either way, ethics and societal expectations must be taken into account.

Recognizing the realities of the 21st Century

Banks should consider social media intelligence as a useful tool for their compliance system in general. According to Article 398 (2) Swiss Code of Obligations, a bank has a duty to gather 'sufficient information' about its client before and during the relationship. One could argue that including social media intelligence into KYC processes is a natural consequence of our digitalizing economy, and is in fact the only way a bank can keep up in the modern world.

The same applies to due diligence obligations in AML regulations. For example, Article 15 (1) AMLO-FINMA stipulates an obligation to gather additional information in high-risk cases. One method mentioned in Article 16 (1) c AMLO-FINMA is to consult publically available sources and databases. In order to meet this requirement, many financial institutions use World-Check. A better use of social media intelligence is valuable to exclude false positive results in a World-Check enquiry. It also provides a new avenue in its own right to verify the plausibility of client information.

There is no silver bullet to prevent the funding of terrorism or other financial crime. But as with other sectors of society, criminals are increasingly active users of social media. The potential for financial institutions to use the resultant intelligence to combat financial crime cannot be ignored.



Blockchain as a solution to KYC challenges

KYC requirements involve the collation of huge volumes of data on every client, as well as continuously monitoring clients to remain vigilant of any changes or emerging risks. As blockchain-enabled solutions gather pace, how can banks use them to carry out this time-consuming obligation?

Undertaking KYC processes can be an onerous task. Three particular problems can lead to excessive financial spend, error-prone audit trails, and long customer onboarding times:

- A silo approach to documentation, where each bank must collect the same client documents and perform separate validation checks
- KYC standards vary between banks and even between branches of international banks, with different types of information being collated and processed
- No single 'source of truth', whereby inconsistent and outdated customer data can lead to problems in identifying possible issues.

Blockchain-based KYC utility – what it is and how it can help

The right solution could go a long way to resolving these three challenges. Namely, through a single source of client due diligence information based on blockchain technology that could be used by a consortium of financial institutions. This would decentralize customer data, with KYC information being accessible to numerous parties with the client's permission. While it would not cover all KYC obligations such as recurring monitoring, this is where technologies such as AI and cognitive processing can help.

The results would be an improvement in efficiency, reduction in costs, and an enhanced customer experience. This would be achieved through data being immutable (it cannot be changed following its creation), encrypted, transparent and consistent between banks.

Also through a reduction in operational inefficiencies with cost savings in KYC onboarding; a reduced risk of financial crime by maintaining real-time up-to-date customer data and a single source to be updated; and by facilitating proof of compliance with regulations, as the data held on the platform would be fully auditable.

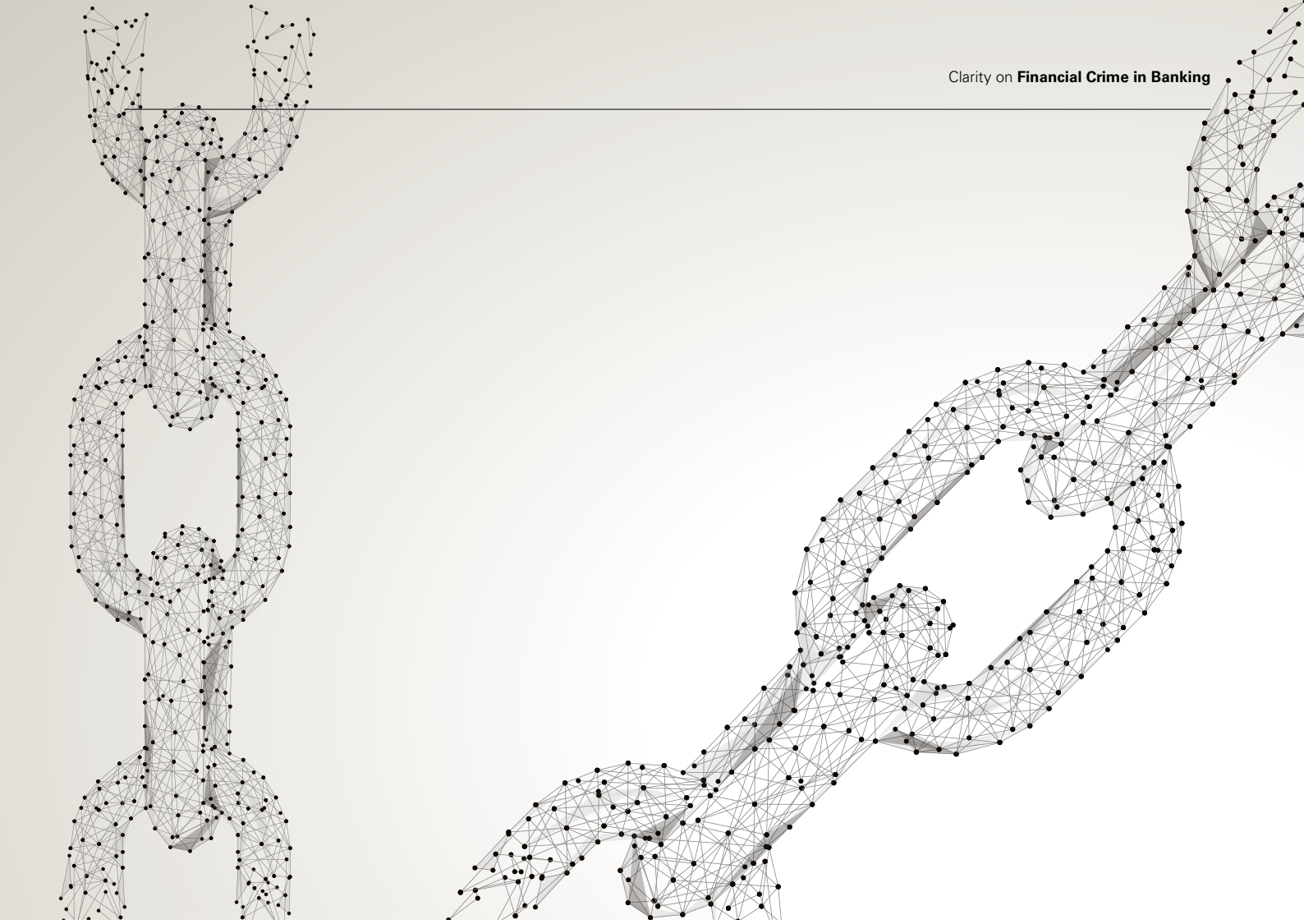
Of course, two obstacles to this solution exist. One is the difficulty of obtaining consensus on due diligence requirements among banks that have their own policies, procedures and risk appetites. And secondly how such a model would comply with Swiss banking secrecy legislation, data protection and privacy regulations.

Practical experience of blockchain-based KYC tools

The past year has seen several collaborations between financial institutions to launch a proof-of-concept of shared KYC projects. There are also authority-driven pilot projects such as the Monetary Authority of Singapore's drive to innovate the country's finance infrastructure while enhancing transparency over banks' KYC processes.

Not just a theory: Singapore's pilot project

This is a proof-of-concept prototype that tested the technical aspects of a blockchain platform in early to mid-2017. It was a collaboration between the Singaporean financial regulator, a consortium of three major banks, and a firm specializing in blockchain technology.



The process was that all new KYC requirements were first queried on the shared platform and any existing customer details shared with the customer's consent. Customer information was validated by third-party sources, with results recorded in the KYC shared ledger. Meanwhile, all actions, permissions and new data provided by customers or participating banks were tracked and recorded.

In the view of KPMG Singapore, the platform remained stable and responsive and performed strongly; data were considered secure and confidential; the platform resisted tampering by third parties; and it provided estimated cost savings of between 25% and 50%. The participating banks meanwhile cited the platform as being able to improve overall efficiency, reduce time to complete necessary screening, improve responsiveness to customers' needs, and reduce the risk of financial crime.

The possible answer to KYC challenges for both banks and clients

KYC requirements are increasingly demanding, and make it more difficult for banks to win and onboard new clients. But it is not only the banks that are challenged: the complexity also manifests itself in seemingly endless form filling by prospective clients. KYC can be extremely inefficient, with many banks spending resources that could potentially be better focused on truly problematic KYC cases.

As the uses of blockchain expand exponentially, the benefits in terms of efficiency, cost and improved customer experience could lead directly to an increase in client satisfaction rates. So while blockchain-based KYC solutions might not be a panacea for all KYC issues, it might be used in combination with technologies such as AI and cognitive processing to introduce considerable improvements for clients and banks alike.

Joint effort: cooperation as the key to combating financial crime

Moves are underway to change some aspects of how public prosecutors can handle data, significantly impacting on collaboration with foreign authorities. At the same time, the MROS is being inundated by a huge surge in the number of reports from Swiss financial institutions. We discuss this and more with:

Bernhard Hecht, Public Prosecutor and deputy to the Head of the Department for Legal Assistance, Money-Laundering Offenses and Asset Forfeiture of the Prosecutors Office of the Canton of Zurich

Daniel Tewlin, former Public Prosecutor with experience in prosecuting white-collar crimes, and former representative of the judicial and prosecution authorities of the Canton of Zurich involved in the FATF meetings concerning the 2016 country report Switzerland

Arnaud Beuret, Lawyer at Bratschi AG law firm in Bern, former deputy to the Head of the Money Laundering Reporting Office Switzerland (MROS) and representative involved in the meetings concerning FATF and the 2016 country report Switzerland

KPMG *One of the criticisms in the FATF country report was the relatively few cases reported in Switzerland. Yet, over the past few years, the MROS has seen a significant uptick in suspicions of money laundering reported by financial institutions. Is this a reaction to the criticism, and what impact does it have on the MROS?*

Beuret Certainly, one of the reasons is that Switzerland has been repeatedly criticized at the FATF meetings for its low number of reported cases in the last and penultimate evaluation round. It is difficult for this commission to understand why a country with such an important financial center reports so few cases. Canada had almost 25 million reported cases in the 2016-2017 year, while Switzerland only had 3,000. An important reason is that the authorities always stated that financial institutions should act as a first filter and the authorities as a second one. Moreover, banking secrecy has been heavily diluted. These days, there are in practice only two conditions to be met before a case can be reported: The existence of an element of suspicion and that the report is bona fide. The threshold for reporting a case has been set extremely low.

At the annual media conference in April 2016, Mark Branson, CEO of FINMA, stated that financial institutions must file a report if any doubt exists. This changed the right to report to a duty to report. He also stated that it was not sufficient if financial intermediaries only filed reports once the press was aware of a case. Nowadays, a large proportion of reports are triggered by press releases. However, increasing the quantity does not necessarily improve the quality. Financial intermediaries have lodged so many more reports within a brief time that the MROS can no longer cope. This should be seen as a loss of quality.

Hecht Another difficulty is the different quality standards. Banks have lowered their criteria for an event to be deemed suspicious, so they also report cases faster than they would have done previously. The prosecution authorities, however, can only open an investigation if there are reasonable grounds for suspicion. This means that the MROS has to increase the threshold of suspicions to ensure it is worth passing a case to the public prosecutor, as the case would otherwise be dropped.

«Increasing the quantity does not necessarily improve the quality. Financial intermediaries have lodged so many more reports within a brief time that the MROS can no longer cope. This should be seen as a loss of quality.»

Arnaud Beuret

The number of SARs submitted under Article 9 AMLA rose by more than 96% according to the MROS's Annual Report 2017. If a financial institution reports a case under the duty to report regime, it has to be handled within 20 days. Whereas a report under the right to report regime may remain untreated for months if not years. What do you think of this trend?

Beuret Banks understand the new regime. Reports made under the duty to report regime receive priority treatment. The MROS's ultimate interest is mainly whether a report was filed and what has been reported. The MROS has a very good database. The important thing is that the data are collected there. Therefore, a prioritization should not be based on formalities but only after a material assessment has taken place.

According to the MROS Annual Report 2016 there were 500 unresolved reports pending at the end of 2016. At the end of 2017, it was 1,423 SARs, including 116 SARs received in 2016. How does the MROS deal with this?

Beuret The MROS currently has 35 employees, up from six employees for years. It tries to add value to the reports to overcome the threshold of reasonable suspicion, so that the prosecution authorities can handle the case. However, if there are even more reports going forward, the MROS cannot guarantee its current level of quality. It is a valid question whether more reports mean added value.

Hecht The MROS's objective should be to provide us with information that allows us to skip the lengthy suspicion review process or preliminary investigations. There has been no increase in headcount at the public prosecutor's in the past few years. By restructuring internally, we cleared some of the backlog. If the MROS opens the floodgates we would probably no longer be able to deal with everything at the public prosecutor's office. As a result, we would have to notify banks that they should stop submitting reports due to the backlog. That would be a disaster.

Cooperation between Swiss authorities and internationally are increasingly important. Until recently, the MROS was not permitted to exchange financial information with foreign financial intelligence units or FIU. Since the revision of the Anti-Money Laundering Act in 2013 the MROS may transmit such financial information in the course of administrative assistance, which is

pivotal to allowing analyses and the preparation of criminal proceedings. However, under the current law, the MROS cannot make available any data for which no Swiss financial institution has submitted a report. There are efforts in the wings to change this: In June 2017, the Swiss Federal Council published a draft on the implementation of the agreement and the Council of Europe's additional protocol on the prevention of terrorism and organized crime. The draft foresees an adjustment of the Anti-Money Laundering Act (draft Article 11a (2bis) and 3 AMLA) that allows the MROS to request information from financial institutions based on a request of a foreign FIU. Could you give us more information on the revision attempts and explain the importance and consequences of the MROS's new competence?

Beuret Many adjustments to the AMLA were made to prevent the international community of financial intelligence units from terminating the MROS's membership due to it having been the only financial intelligence unit hampered by banking secrecy from passing on financial data. Simultaneously, the currently applicable Article 11a AMLA was added. Article 11a (1) AMLA already reflected current practice. Contrary to this, Article 11a (2) AMLA was revolutionary because now the MROS can obtain information from a non-reporting financial intermediary that pertains to a report. Today, the community is of two minds as to whether such an information request constitutes an order. The argument seems to be in favor, especially if we look at the definition of an order. The dispatch on the AMLA as well as the authorities are of the opinion that this constitutes only an invitation to make documents available; thus, there are no means of legal redress. In the meantime, the debate is concentrating on whether Article 11a should be expanded to allow the MROS to obtain data from financial intermediaries because of information or a request from abroad. A legal expansion in regard to the exchange of financial data would be ideal for the MROS, but the question is whether this would be constitutional and whether it would indeed improve the efficiency.

Pascal Sprenger, KPMG

Franziska Balsiger, KPMG

Hecht Regarding administrative assistance, we encounter two issues. First, our work focuses on procuring evidence on behalf of foreign judicial proceedings. When looking at requests for administrative assistance, we realized that they often pertain to earlier stages than that. It is no longer a question of reviewing documents that will later serve as evidence. Rather, we are asked to actively support investigations, for instance by implementing surveillance measures. We can order covert surveillance based on a request for administrative assistance but the problem is that it will not remain secret. According to the current Mutual Assistance Act and the most recent practice by the Swiss Federal Court, I am obliged to inform the person affected beforehand.

According to the current law, data on let's say a monitored telephone line may not be divulged unless the person monitored knows that he has been monitored and only if he agrees to these data being released or after he has contested its release at the Swiss Federal Supreme Court and has lost. Wiretapping a telephone line is an extreme case, but the problem already starts with bank documents. Foreign authorities cannot understand that we can issue a communication ban only until the point in time of the decision to surrender the documents. It would be an important step if we had the possibility to release data not as evidence but rather in support of investigations. This would require that we would be notified once the information will be used as evidence so that we could inform the person affected in order to protect that person's rights to appeal.

«We can only maintain a good reputation if we work together, that is privately by financial institutions, among regulators and by prosecutors.»

Bernhard Hecht

The amount of data to be processed and the technologies with which financial crimes are being committed is becoming more complex. What are your biggest challenges in this regard?

Hecht The amount of data is a challenge, especially with regard to costs. If I have to search for information on a hard disk one terabyte large, which is quite standard these days, this may cause difficulty. This is also why we are restructuring the public prosecutor's office. White-collar crimes are becoming more and more international. Up to now, there was a segregation between international administrative assistance and the Public Prosecutor's Office 3 that is responsible for handling white-collar crimes. As of July this year, these two departments will be merged. This will help to bundle our knowledge. A large part of our work in international administrative assistance concerns major cases of white-collar crime where we assist foreign authorities. If we place a request for administrative assistance abroad, we will now have in-house specialists with whom this data may be exchanged. This will give us more clout.

Some Swiss banks have set up a whistleblower hotline, others are thinking of doing so. But a KPMG

study shows that whistleblowing does not yet play much of a role in detecting white-collar crimes at banks. How important do you believe hotlines are in detecting rule violations?

Tewlin I do see advantages and would like to refer to the FATF report. One of the criticisms was the implementation of preventive measures by financial intermediaries. The creation of such an internal hotline would be a suitable preventive measure to improve the image of Swiss financial intermediaries. There are other aspects, such as a case of a senior manager supposedly embezzling funds. A person reporting to the senior manager detected this and feared losing his job if he were to inform his direct line manager. I discussed the employee's dilemma with the Chairman of the Board of this group at the time. The Chairman assured me that he would introduce whistleblowing and that he would make sure that this person did not experience any sanctions. Further, he assured us that future employment agreements would include that whistleblowing does not lead to employment disadvantages or termination. This pilot case caused quite a bit of international excitement. Such a hotline should not necessarily be seen as competition to the internal Compliance department. It is more an additional tool.

Many banks I spoke to during our study felt that their employees did not pose a great risk. Perhaps the institution perceives the value of a whistleblower hotline to be negligible?

Tewlin That may well be an explanation. I had another focus because I headed the department that specifically handled white-collar crimes. Generally, employees that tried to line their own pockets were those responsible for departments, who had access rights and the right to give instructions, and who could give orders that were not questioned or verified by others. It should be in the interests of financial institutions to implement hotlines to prevent such cases. Simply having a whistleblower hotline can have a positive effect on a bank. As well as detecting cases, an advantage is the information gained. In many cases, it makes sense to speak to the prosecution authorities before filing a crime report. In this way, the bank is in the driver's seat as far as the criminal procedure is concerned. However, if the case starts from the outside, the bank will experience pressure, either by us or investigative journalists.

> «It should be in the interests of financial institutions to implement hotlines to prevent such cases. Simply having a whistleblower hotline can have a positive effect on a bank.»
>
> **Daniel Tewlin**

How should a company prepare itself in order to best support the prosecution authorities and why is this also in the interest of the company?

Tewlin In complex cases that are international, such as the transfers to Panama, where these funds are then hidden within some kind of constructs, high quality and comprehensive documentation is important. It should have no gaps with regard to the incriminating flow of funds. Readying such data, possibly in electronic form, is advantageous. In this regard it might also make sense to find out which types of data the police and public prosecutor in question can read and process. An executive summary is also helpful, especially for the persons responsible for the investigations. It is certainly also beneficial to look at who is in charge of what at the prosecutor's office.

Do you have a final message to the Swiss financial industry to make the combating of white-collar crime more efficient?

Hecht The title of the interview already says a lot: 'joint effort'. Everyone's objective should be that, together, we provide a clean financial center. Switzerland's financial center is vital for the country's economy and reputation. Over the past few years, this has become a bit tattered. We can only maintain a good reputation if we work together, that is privately by financial institutions, among regulators and by prosecutors. If we do not collaborate properly and transparently, we will never reach our objective.

Beuret It is difficult if the law and the head of the regulatory authority contradict each other. The crux of the matter lies with the Compliance department whose employees are by nature neither 'fish nor fowl'. Therefore, I would like to end with the same message that I always have at the end of a Compliance training course: Good luck! It might sound trivial but Compliance employees – if they are unlucky – may not have any choice but to be confronted by the public prosecutor. The best way forward is to collaborate.

Benchmark

Find out how your bank's approach to financial crime compares to others in your industry.

Among cantonal banks (11 that participated in the survey)
- Compliance is represented on the Executive Board only in one cantonal bank
- 10 cantonal banks considered 'tone at the top' to be essential for an overall consistent and efficient compliance. No cantonal banks invest in ad-hoc consulting services or other services from third party providers to combat financial crime

Among private banks (14 that participated in the survey)
- Compliance is represented on the Executive Board at the majority
- 13 considered 'tone at the top' to be essential for an overall consistent and efficient compliance
- 6 invest primarily in ad-hoc consulting services or other services from third party providers to combat financial crime

Among foreign-controlled banks (8 that participated in the survey)
- 7 were either satisfied or very satisfied with their current client screening system. 6 were either satisfied or very satisfied with their current CRM system
- 5 stated that extensive client reviews were the major challenge within the past 24 months, and five that the major challenge was increased regulatory expectations

Among regional and savings banks (7 that participated in the survey)
- All said 'tone at the top' is essential for an overall consistent and efficient compliance
- 2 out of 7 were made aware by internal resources of being involved in, or targeted by, a financial crime
- 4 think that complying with formal requirements alone is sufficient to combat financial crime effectively

What is particular about banks that are satisfied with the status quo, how their institution fights financial crime and have no further wishes (7 of 50)?

- The perpetrators of financial crimes affecting banks were exclusively third parties that had no relationship with the bank. Clients or bank employees were not perpetrators of financial crime
- Top-level commitment is central for all these 7 banks
- 5 said they were not satisfied with the client screening system but had no plans to change it
- No bank thinks that they should do more than comply with the official requirements to combat financial crime

Survey methodology

This study is based on a survey of 50 representatives of banks located in Switzerland, being:

– 11 with headcount in excess of 1,000 and
– 39 with headcount of 1,000 or less, of which 21 had headcount of between 100 and 1,000.

The typical respondent profile was member of the Executive Board, department head with responsibility for the organization's legal and compliance, or Compliance Officer.

In addition, interviews were conducted with external subject matter experts on selected topics.

The survey and interviews were carried out by KPMG Switzerland between November 2017 and April 2018.

Contacts

Head Financial Services & ExCom Member

Philipp Rickert
Partner
Head Financial Services

+41 58 249 42 13
prickert@kpmg.com

Philipp Rickert is Head of Financial Services at KPMG Switzerland. He is an accredited lead bank auditor (Swiss Financial Market Supervisory Authority FINMA) and engagement partner of various international clients in the area of private and investment banking. He has extensive expertise in advising national and global financial institutions and is a specialist in accounting and regulation issues for financial institutions.

Head Regulatory & Compliance

Philippe Fleury
Partner
Financial Services
Regulatory & Compliance

+41 58 249 37 53
pfleury@kpmg.com

Philippe Fleury has been Head of Forensics Switzerland since 2014. He specializes in the investigation of fraud, compliance, support in litigation and the fight against money laundering and financial crime at home and abroad. His core competencies also include leading complex investigations into fraud and misconduct and he supports clients in the prevention of such cases.

Governance, Organization & Benchmarking

Pascal Sprenger
Partner
Financial Services
Regulatory & Compliance

+41 58 249 42 23
psprenger@kpmg.com

Pascal Sprenger advises national and international clients mainly in matters of financial market law as well as general contract and company law. His clients are mainly regulated institutions which he also represents in supervisory proceedings towards FINMA. Main topics are questions of internal business organization and governance of regulated institutions, as well as questions of combating money laundering.

Reto Gareus
Partner
Financial Services
Regulatory & Compliance

+41 58 249 42 51
rgareus@kpmg.com

Reto Gareus is an accredited Lead Auditor and has over 10 years of experience providing audit, assurance and advisory services to a variety of financial service firms globally. Reto's area of specialism are core Governance and Compliance topics. He has in-depth experience of Swiss and international regulations, working with global banking clients in the area of wealth management and investment banking and dealing with complex regulatory topics. Reto is a frequent speaker in industry fora.

Financial Crime Framework

Markus Rohner
Director
Financial Services
Regulatory & Compliance

+41 58 249 57 63
mrohner@kpmg.com

In his role as advisor and auditor, Markus Rohner has more than 10 years of experience in the financial crime area. As part of his activities, he is involved in financial crime governance and due diligence aspects such as risk appetite frameworks, organisation, delineation between first and second line activities, consolidated supervision, KYC maintenance, risk classification and transaction monitoring. He focuses on regulatory compliant and pragmatic solutions to elevate institutions' financial crime framework.

Adrian Huser
Director
Financial Services
Assurance & Accounting

+41 58 249 28 34
ahuser@kpmg.com

Adrian Huser is an accredited leading bank auditor (Swiss Financial Market Supervisory Authority FINMA) and has profound experience leading major (special) engagements for both global and national financial institutions. In addition to his client-facing role, he acts as topic owner for auditing anti-money laundering, control and compliance matters and is part of the AML working group of EXPERTsuisse.

Forensic - Fraud & Investigations, client File Reviews

Niko Van der Beken
Partner
Financial Services
Forensic Technology

+41 58 249 75 76
nvanderbeken@kpmg.com

Nico Van der Beken heads the KPMG Forensic Technology Team Switzerland and can look back on over 25 years of work experience in the IT sector. Nico has conducted numerous investigations in connection with fraud, employee misconduct, antitrust violations, corruption, data loss, data breaches, cyber attacks, or regulatory/compliance projects.

MROS Investigation & FINMA Enforcement

Franziska Balsiger
Director
Financial Services
Regulatory & Compliance

+41 58 249 68 77
fbalsiger@kpmg.com

Franziska is a lawyer and member of Regulatory & Compliance at KPMG Switzerland with a focus on Legal & Compliance. Franziska advises national and international clients in various aspects of banking (supervisory) and financial market law and in the area of compliance. She also has broad experience in the area of internal investigations in the banking regulatory environment and complex supervisory procedures.

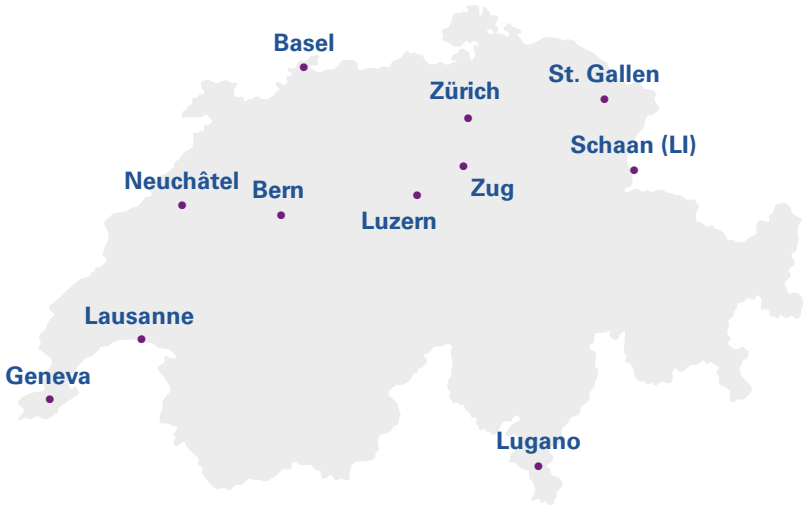
Andreas Hagi
Manager
Financial Services
Regulatory & Compliance

+41 58 249 65 53
ahagi@kpmg.com

Andreas is a specialist in regulatory obligations of banks and internal and external investigations. He advises domestic and foreign corporate clients and private individuals on corporate and financial market law issues. He specializes in regulatory issues in the banking and stock exchange sector, as well as banking supervision law, corporate law and collective investment schemes.

About KPMG

Locations



Revenues by function

Audit	Tax	Advisory
50%	29%	21%

CHF 423,5 million
Total net revenues 2017

More than 2,150 employees
in Switzerland

Of which, 430 employees
in Financial Services

Why KPMG

Market leader in financial services
With a share of 40%, KPMG Switzerland generates the largest revenue in the financial services sector. This is only possible thanks to the broad base of financial institutions that make use of KPMG's auditing and consulting services.

KPMG currently audits over 50 banks and securities dealers, including 5 of the 10 largest banks in the financial services sector. This offers us insights into current and future trends and problems and allows us extensive benchmarking, especially in the area of private and retail banks of all sizes.

Our sector expertise
Thanks to our 430 employees and our multidisciplinary teams in the financial services sector, we are a one-stop shop for you. Especially in the AML area we have access to a repertoire of experts from the areas of Legal, Regulatory, Technology & Compliance.

When it comes to using our technologies there are no interfaces with third parties, which guarantees full independence. For instance, tools such as Astrus give us access to external background information worldwide. These Astrus Reports disclose relationships between companies and private individuals and identify clear risk indicators.

Our services

Governance Framework

Risk appetite
- Development and review of risk appetite statements/limits for clients, markets, products including, for example, cryptocurrencies

Governance & organization
- Assessing the compliance organization, defining target operating model and capacity planning/rebalancing the work between the first and second line of defense

Consolidated supervision
- Review and enhance the group supervision framework

Risk and Information Management Framework

Management reporting
- Review and assessment of financial crime management information

Risk analysis
- Review and assessment of the risk analysis (risk limits) including reporting to those charged with governance

Due Diligence Framework

KYC maintenance
- Review and remediation of PEP/High risk and normal risk accounts, including review and tracking of KYC change in circumstances
- Review, improvement and benchmarking of the KYC template

Risk classification
- Review and enhancement of the client risk classification model

Transaction monitoring
- Review of high risk transactions/treatment of alerts
- Investigation into transactions that were not compliant with the sanctions list
- Review and assessment of transaction monitoring effectiveness, including remediation to reduce false/positive alerts

Data analytics
- Data analytics to uncover patterns of financial crime

Robotics Process Automation
- Retrieve customer and counterparty data from internal systems, external sites upon prescribed procedures to automate highly repetitive manual alert resolution tasks

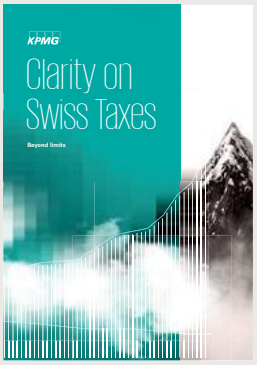
Machine learning
- Enhancement of monitoring rules by enabling the use of structured/unstructured data to support elements of self-learning
- Improvement of sanction alert classification by implementing machine learning routines

"Clarity on" publications

This series of publications from KPMG Switzerland provides insights, analyses and studies on a range of topics. All publications are available online. For more information, please contact **kpmgpublications@kpmg.com**

Latest issues

Clarity on
Cyber Security

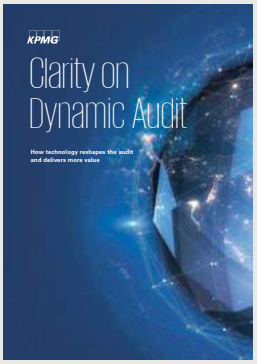


Clarity on
Swiss Taxes

Clarity on
Mergers & Acquisitions

Clarity on
Digital Labor

Clarity on
Performance of Swiss Private Banks



Clarity on
Dynamic Audit

Clarity on
Insurance Digitalization

Clarity on
kpmg.ch/clarity-on

KPMG Knowledge App

Get instant access to our experts' knowledge with our KPMG Knowledge App for iPad, iPhone and Android phone.

Download on the App Store

GET IT ON Google Play

CONTACTS & IMPRINT

For further information on
Clarity on
Financial Crime in Banking
please contact:

Philipp Rickert
Partner, Head of Financial Services,
Member of the Executive Committee
+41 58 249 42 13
prickert@kpmg.com

Pascal Sprenger
Partner, Financial Services,
Regulatory & Compliance
+41 58 249 42 23
psprenger@kpmg.com

Philippe Fleury
Partner, Financial Services,
Regulatory & Compliance
+41 58 249 37 53
pfleury@kpmg.com

Franziska Balsiger
Director, Financial Services,
Regulatory & Compliance
+41 58 249 68 77
fbalsiger@kpmg.com

Publisher
KPMG AG
Badenerstrasse 172
PO Box
CH-8036 Zurich
+41 58 249 31 31
kpmgpublications@kpmg.com

Study and editorial team KPMG
Franziska Balsiger
Renata Pagnamenta
Pascal Sprenger

Concept and design
Irene Hug, KPMG
Sabine Lorencez, KPMG
Andi Portmann, Grafikagentur konkret

Print
PrintCenter Hergiswil

Pictures
Shutterstock
iStock
Getty Images

[Page 59–60]
Louis Rafael Photography

[Page 71–74]
Daniel Hager Photography & Film GmbH

Illustrations
[Page 1]
van Beusekom design & brand solution

MIX
From responsible sources
FSC® C010670
www.fsc.org

PERFORMANCE
myclimate
neutral
printed matter
No. 01-14-569853 – www.myclimate.org
© myclimate – The Climate Protection Partnership

Clarity on Financial Crime in Banking
kpmg.ch/financialcrime