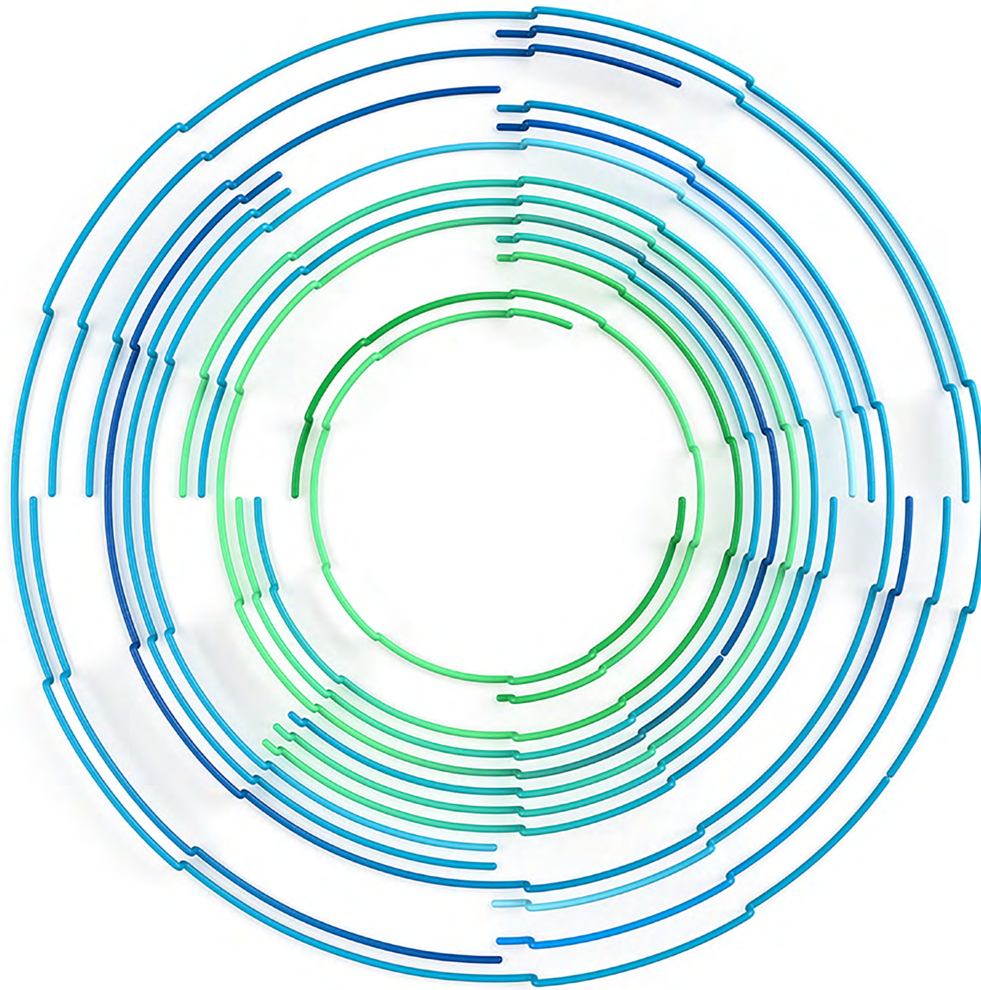


Financial Crime Due Diligence

Assessing banks or institutions for their risk of exposure to financial crime can point towards the organization's vulnerability, as shown in numerous events in the past. The global COVID-19 pandemic has caused financial institutions more concerns and risks to be exposed to frauds, scams, and other financial crimes. This unprecedented crisis even more assures that financial entities should adopt stringent due diligence measures to safeguard their data and resources.

In recent years, regulators have drastically stepped up enforcement against financial crimes, such as violations of sanctions and anti-money laundering (AML) laws and regulations. It is not uncommon to see regulators in many jurisdictions announce criminal or civil fines amounting to several million, or even billion, euros as punishment for financial crimes.

A number of significant money laundering cases have become public, including the Russian/Azerbaijan Laundromat, the Panama and Paradise Papers, and the Danske Bank scandal. These cases, and others like them, show both the scale and complexity of money laundering schemes and the ease with which the proceeds of crime can be transferred between different jurisdictions. The integrity of our financial system is at risk.

The patterns and red flags relating to financial crimes are now emerging. Findings issued by the Dutch regulator in their report regarding a Dutch financial institution describe the weaknesses and deficiencies in the bank's AML Compliance Program, which may also be highly relevant for other banks and demonstrate the importance of strong, efficient, and robust compliance systems.

Financial crime topics not only concern the safety and soundness of business-as-usual operations. For Mergers and Acquisitions (M&A) transactions, conducting financial crime due diligence for risk assessment purposes is an integral element. Caveat emptor ("Let the buyer beware"), the old principle that buyers are responsible for checking the quality and suitability of goods before purchase, explains how crucial financial crime due diligence is when an organization is involved in M&A deals. It is your responsibility to check that what you are buying can be trusted and is free of ill-gotten gains or hidden risks.

Regulators have increasingly become vigilant in pursuing their concerns over potential financial crime risks accompanying M&A transactions. Appropriate risk assessments that include AML, sanctions, and other regulatory risks help organizations detect potential risks, regulatory violations, and systematic deficiencies. This paper explores the heightened awareness of financial crime due diligence alongside M&A transaction scenarios as well.

Relevant Laws, Regulations, and Guidelines

Banks are faced with a comprehensive set of regulations, best practices, and guidance papers that outline the standards concerning risk management as it relates to anti-financial crime programs. Here are some of the relevant laws, regulations, and guidelines for financial entities subject to the EU and US jurisdictions:

- Global: Basel Committee on Banking Supervision: Sound management of risks related to money laundering and financing of terrorism[1]
- EU: Directive 2015/849, supplemented by Directive (EU) 2018/843[2]
- EU: Regulation on information accompanying transfers of funds (EU) 2015/8473[3]
- US: US Department of Justice (DOJ): Evaluation of Corporate Compliance Programs[4]
- US: US Department of the Treasury, Office of Foreign Assets Control (OFAC): A Framework for OFAC Compliance Commitments[5]
- EU: ECB Guide on the supervisory approach to consolidation in the banking sector[6]

Financial crime topics not only concern the safety and soundness of business-as-usual operations. For Mergers and Acquisitions (M&A) transactions, conducting financial crime due diligence for risk assessment purposes is an integral element.

[1] Basel Committee on Banking Supervision: https://www.bis.org/bcbs/publ/d353.pdf
[2] EU Directive 2015/849: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32015L0849
[3] EU Regulation 2015/847: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32015R0847&from=DE
[4] U.S. Department of Justice (DOJ) Criminal Division: https://www.justice.gov/criminal-fraud/page/file/937501/download
[5] U.S. Department of the Treasury, OFAC: https://www.treasury.gov/resource-center/sanctions/Documents/framework_ofac_cc.pdf
[6] ECB Guide on the supervisory approach to consolidation in the banking sector (Public consultation): https://www.bankingsupervision.europa.eu/legalframework/publiccons/html/consolidation.en.html

Main areas of application

What are the objectives of conducting a financial crime due diligence project? There are two main reasons why a financial crime due diligence program is important:

- **(1) Health check:** conducting a regular or ad hoc risk-based "health check" through a third party for your organization's financial crime program and related risks.
- **(2) M&A situations:** conducting an ad hoc focused risk assessment for specific entities in an M&A transaction in order to identify risk areas related to financial crime with potential impact on pricing and structuring of the M&A deal.

(1) Risk-related health checks for business-as-usual operation

Performing regular or ad hoc financial crime due diligence reviews is prudent and essential to your organization's day-to-day operation. It is about "health check," assessing your entity's current status of overall health, such as risks of financial crimes, financial crime-related programs, and areas for potential remediations.

This organizational health check can be conducted by an independent third-party consultant. For example, when a new management team comes onboard, financial crime due diligence performed by an independent and impartial third party is crucial for diagnosing and evaluating the company's risk environment, risk appetite, and risk-related controls and learning how prepared the company is for risk-taking in pursuit of strategic objectives as well as minimizing risk in line with the company's policies, controls, and financial crime management.

Effective financial crime programs can mitigate potential fines

In the US, the importance of having an effective compliance program that relates to the organization's daily operations has been emphasized since the early 1990s. Like individuals, US organizations can be found guilty of criminal conduct such as fraud, tax offenses, and antitrust offenses, and they can be fined, sentenced to probation, or ordered to make restitution when found guilty.

The US Sentencing Commission has promulgated the organizational sentencing guidelines since 1991, which includes how having an "effective compliance program" in place can mitigate the potential range of fines, in some cases up to 95 percent. Below is a list of the Commission's key criteria.

US Federal Sentencing Guidelines for Organizations
(US Sentencing Commission)

Key criteria for establishing an "effective compliance program":

Compliance standards and procedures reasonably capable of reducing the prospect of criminal activity

- Oversight by high-level personnel
- Due care in delegating substantial discretionary authority
- Effective communication to all levels of employees
- Reasonable steps to achieve compliance, which include systems for monitoring, auditing, and reporting suspected wrongdoing without fear of reprisal
- Consistent enforcement of compliance standards including disciplinary mechanisms
- Reasonable steps to respond to and prevent further similar offenses upon detection of a violation[7]

In Germany, the "Verbandssanktionen-gesetz" currently being drafted is expected to provide new guidance on the topic of how effective compliance measures will mitigate potential fines in Germany.

[7] United States Sentencing Commission: https://www.ussc.gov/sites/default/files/pdf/training/organizational-guidelines/ORGOVERVIEW.pdf

(2) Price-related checks in M&A situations

When a company buys another company, considerable analysis must be performed to assess the overall value of the target company, including its financial performance, the quality of its assets, risk areas including risk management practices, and its compliance programs. Unfortunately, some companies may hide past or current violations or financial crimes. As a buyer, you will want to know, for instance, whether there have been ill-gotten profits, hidden financial crime risks, potential or active authorities' enforcement actions, or payments of penalties.

Unbeknownst to you as a buyer, these violations and crimes can become your responsibility when you close M&A deals and result in damage to your reputation, ensuing litigation, and constraints or limitations on your business operations or specific risk areas (e.g., sanctions exposure) after the deal is closed. This is why financial crime due diligence is necessary to help you avoid these pitfalls and risks during M&A transactions, or to pay the price later.

One example of financial crime risk areas in M&A deals is the OFAC's sanctions list. This ensures that all the trade and sanctions regulations applying to the target company are respected and complied with. OFAC-related sanctions risk assessment and any program weaknesses found are particularly important for US buyers, since a proper evaluation of sanctions risk exposure has a significant impact on the price the buyer must pay when acquiring the target company, as well as on additional obligations after the deal is closed. Other examples of risk areas are anti-money laundering risk, anti-bribery risk, corruption, and fraud.

With respect to US sanctions-related due diligence, OFAC published its first-ever "Framework for OFAC Compliance Commitments" on May 2, 2019. OFAC clearly stated that it will consider "favorably" if companies have effective sanctions compliance programs in place when resolving enforcement cases. The OFAC Framework highlights the importance of conducting a sanctions risk assessment for mergers and acquisitions. Please see below what OFAC states.

Mergers and Acquisitions (M&A)
[...] proper risk assessments should include and encompass a variety of factors and data points for each organization. One of the multitude of areas organizations should include in their risk assessments—which, in recent years, appears to have presented numerous challenges with respect to OFAC sanctions—are Mergers and Acquisitions. Compliance functions should also be integrated into the merger, acquisition, and integration process. Whether in an advisory capacity or as a participant, the organization engages in appropriate due diligence to ensure that sanctions-related issues are identified, escalated to the relevant senior levels, addressed prior to the conclusion of any transaction, and incorporated into the organization's risk assessment process. After an M&A transaction is completed, the organization's Audit and Testing function will be critical to identifying any additional sanctions-related issues.[8]

Recently, on June 1, 2020 the US Department of Justice (DOJ) published its updated Corporate Compliance Program guidance, where the department emphasizes the importance of due diligence for pre- and post-M&A due diligence as part of a company's compliance programs: "Pre-M&A due diligence, where possible, enables the acquiring company to evaluate more accurately each target's value and negotiate for the costs of any corruption or misconduct to be borne by the target. Flawed or incomplete pre- or post-acquisition due diligence and integration can allow misconduct to continue at the target company, causing resulting harm to a business's profitability and reputation and risking civil and criminal liability."[9] DOJ also includes several factors for the prosecutors to consider when assessing corporate compliance programs:

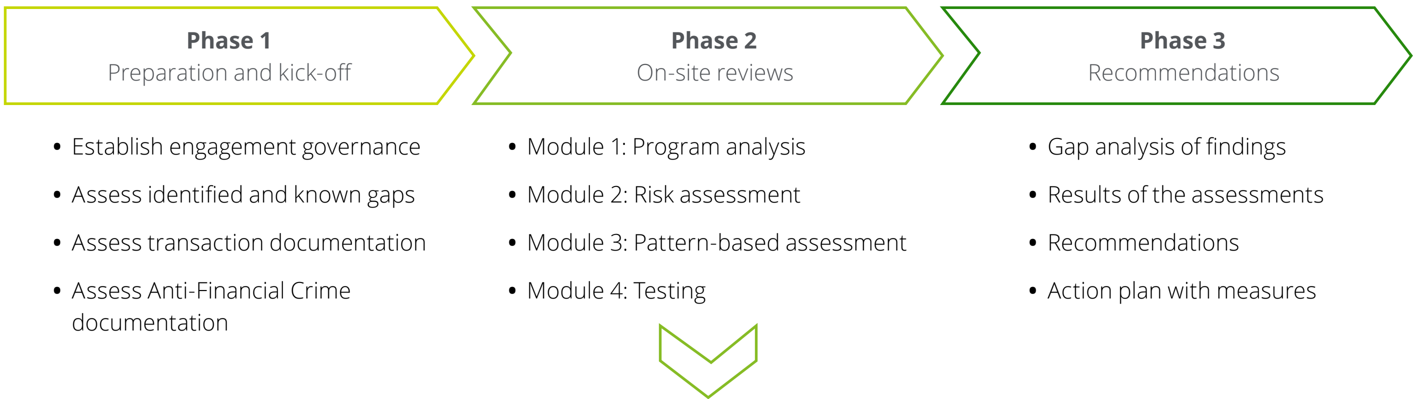
Due Diligence Process –
Was the company able to complete pre-acquisition due diligence and, if not, why not? Was the misconduct or the risk of misconduct identified during due diligence? Who conducted the risk review for the acquired/merged entities and how was it done? What is the M&A due diligence process generally?

Integration in the M&A Process –
How has the compliance function been integrated into the merger, acquisition, and integration process?[10]

[8] U.S. Department of The Treasury, OFAC: https://www.treasury.gov/resource-center/sanctions/Documents/framework_ofac_cc.pdf
[9] U.S. Department of Justice (DOJ): https://www.justice.gov/criminal-fraud/page/file/937501/download
[10] Ibid.

Three-phase approach of financial crime due diligence

The following chart describes Deloitte's three phases in performing a financial crime due diligence program. Phase 1 starts with establishing engagement governance and assessing the status of identified gaps. In phase 2, predefined work and on-site assessments are performed. Phase 3 delivers a gap analysis, findings, and recommendations.



- Establish engagement governance
- Assess identified and known gaps
- Assess transaction documentation
- Assess Anti-Financial Crime documentation

- Module 1: Program analysis
- Module 2: Risk assessment
- Module 3: Pattern-based assessment
- Module 4: Testing

- Gap analysis of findings
- Results of the assessments
- Recommendations
- Action plan with measures

Phase 2 modules include:

Module 1
Program analysis

Program analysis focuses on assessing the completeness and adequacy of the organization's key components in its financial crime program, including written documentation and controls.

Module 2
Risk assessment

Risk assessment concerns how the organization has implemented a risk-based approach, including its risk assessment and risk rating methodologies and processes, the risk appetite framework and statement, and how specific risks are translated into effective controls.

Module 3
Pattern-based assessment

Pattern-based risk exposure assessment includes "outside-in" pattern-based analysis on whether the organization's business model bears the risk of being used as a vehicle for money laundering, for example. The following relevant key areas are analyzed:

- Implemented risk categorization
- Non-resident clients portfolio
- Offshore/high-risk countries/PEP relationships
- Legal forms such as Ltd., PIC, LLP, or LLC
- Correspondent banking, international payment activities

Module 4
Testing

Testing focuses on two key areas to identify potential risks related to the business, such as transition activity analysis and KYC file review.

- Transaction activity analysis: the objective of transaction activity analysis is identifying obvious matches in transactions and client records between bank-related entities, customer and originator/beneficiary records of cross-border transactions, and entities mentioned on selected sanction lists (EU, UN, OFAC), as well as publicly available information concerning financial crime schemes.
- KYC file review: KYC file review is sample-based and assesses the bank's customer due diligence standards and execution quality with respect to KYC regulatory requirements.

Conclusion

Financial crime due diligence plays a crucial role, both in conducting risk-focused health checks for an organization's business-as-usual operations and in M&A situations.

In light of ever-increasing regulatory emphasis and enforcement actions regarding financial crimes globally, assessing and understanding your risk of exposure to financial crime has become an integral part of your organization's success.

Having efficient financial crime due diligence should be regarded not only as a prudent and essential check-up for your company's health, but as a substantial and worthwhile process in your M&A transactions as well.

Deloitte is here to help you perform health and readiness checks for financial crime due diligence.

Contact

Matthias Rode
Partner | Forensic
Tel: + 49 (0)151 58002270
mattrode@deloitte.de

Dr. Andreas Burger
Partner | Forensic
Tel: + 49 (0)151 58076486
anburger@deloitte.de

This communication contains general information only not suitable for addressing the particular circumstances of any individual case and is not intended to be used as a basis for commercial decisions or decisions of any other kind. None of Deloitte GmbH Wirtschaftsprüfungsgesellschaft or Deloitte Touche Tohmatsu Limited, its member firms, or their related entities (collectively, the "Deloitte network") is, by means of this communication, rendering professional advice or services. No entity in the Deloitte network shall be responsible for any loss whatsoever sustained by any person who relies on this communication.

Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited, a UK private company limited by guarantee ("DTTL"), its network of member firms, and their related entities. DTTL and each of its member firms are legally separate and independent entities. DTTL (also referred to as "Deloitte Global") does not provide services to clients. Please see www.deloitte.com/de/UeberUns for a more detailed description of DTTL and its member firms.

Deloitte provides audit, risk advisory, tax, financial advisory and consulting services to public and private clients spanning multiple industries; legal advisory services in Germany are provided by Deloitte Legal. With a globally connected network of member firms in more than 150 countries, Deloitte brings world-class capabilities and high-quality service to clients, delivering the insights they need to address their most complex business challenges. Deloitte's approximately 312,000 professionals are committed to making an impact that matters.

Issue 09/2020