Developing a Corporate Protocol for Investigating AML/Sanctions-Related Misconduct

CAMS-Audit Advanced Certification White Paper ACAMS

Beate Prochaska, 11 March 2019

DISCLAIMER

The opinions and views of this white paper only express the author's thoughts and do not necessarily reflect the opinions of her employer.

Table of Contents

1. Executive Summary

"When a culture of compliance is lacking, the result is ineffective AML safeguards."[1]

One of the pillars of an effective anti-money laundering (AML)/sanctions compliance risk management is the establishment of a sound risk culture in the context of regulatory compliance, known as compliance culture.

Compliance culture, on the one hand, requires defining expectations in regard to compliance with external and internal requirements, and incentivizing desirable behavior and actions within the organization. On the other hand, it also requires a clear protocol for investigating and sanctioning misconduct, especially when AML and/or sanctions breaches have occurred. Having a clearly defined and consistent protocol for investigating misconduct in place is much more than a formal requirement; it is evidence of the financial institution's integrity.

Over the last years, literature on the topic of compliance culture, as well as workplace investigations, has been emerging. Still, these two topics so far have not been discussed together. The intention of this white paper is to close this gap and highlight the synergies.

The objective of this white paper is to detail the key considerations in developing a corporate protocol for investigation of AML/sanctions-related misconduct. As a starting point, it provides a definition and classification of "misconduct." On this basis, the conduct investigation lifecycle is detailed from the identification of relevant cases to the reporting of the results and referral for decision on disciplinary action. The last section looks at standards and governance aspects to be considered in the allocation of responsibility for performing investigations of potential misconduct.

This white paper uses AML/sanctions as an example and makes reference to specific aspects relevant for the AML/sanctions compliance and audit function in the financial institution. However, it can also be applied to any other area of compliance.

2. Conduct Investigations in the Context of Compliance Culture for AML/Sanctions

While AML and sanctions compliance are a relatively young area of laws and regulations, they have already been subject to noteworthy evolution. It started with a prescriptive approach in the 1970s and developed into the principle, and subsequently risk-based approach, in the late 2000s.[2] In further development, culture became an additional dimension to an effective AML/sanctions risk management to ensure that revenue concerns do not lead to compromises over

[1]See Shasky Calvery, Jennifer. (2013). Remarks of Jennifer Shasky Calvery, Director Financial Crimes Enforcement Network.
[2]See Financial Action Task Force. (2007). *Guidance on the Risk-Based Approach to Combating Money Laundering and Terrorist Financing.*

compliance, or that red flags are overlooked because someone is a good customer or the account is generating substantial fees.[3]

In its 2014 "Advisory to U.S. Financial Institutions on Promoting a Culture of Compliance,"[4] the Financial Crime Enforcement Network (FinCEN) states: "FinCEN seeks to highlight the importance of a strong culture of BSA/AML [Bank Secrecy Act/Anti-Money Laundering] compliance for senior management, leadership and owners of all financial institutions (…) regardless of size or industry sector."

The advisory provides guidance on six components that strengthen financial institutions' BSA/AML culture. The named components are targeted to set clear expectations for financial institutions on complying with BSA/AML requirements and setting the framework for a robust BSA/AML program.

For the BSA/AML/sanctions culture to become reality for a financial institution's employees, more is required than setting expectations and a framework. To create credibility, it is necessary to create accountability. For S. Chris Edmonds,[5] there are three steps to holding people accountable, which are: (1) clear expectations; (2) proactive observation; and (3) consequence management. Translating this for the AML/sanctions program means that in order for the program to be taken seriously and staff to assume accountability, a consequence management process needs to be established. This means positively rewarding and incentivizing correct behavior, but also taking action when misconduct occurs.

In order for the sanctioning of a case of misconduct to be fair and consistent, it is important to fully identify the facts and circumstances of the breach and assess accountability. To achieve these goals, an independent investigation is required, and this will be referred to as a conduct investigation. For the purpose of this white paper, the definition of a conduct investigation will be: a special investigation with the aim to identify the facts and circumstances of the potential misconduct and to establish the accountability for confirmed misconduct.

The importance of consequence management and handling cases of misconduct also becomes apparent in the U.S. Department of Justice's Evaluation of Corporate Compliance Programs in the context of Fraud.[6] The first category of Sample Topics and Questions relates to Analysis and Remediation of Underlying Misconduct, requiring a root cause analysis, and looking at prior indications and the resultant remediation. This shows that there is a clear expectation that the financial institution has performed its own analysis of the misconduct.

The value of investigating misconduct, however, goes beyond identifying the responsibility for past breaches. It also is a tool to improve risk management and business operations going forward by, amongst others, identifying areas of increased

[3]See Moskow-Schnoll, B. (2018). *Practical Tips for Ensuring Your AML Program Withstands the Scrutiny of Regulators.*
[4]See Financial Crimes Enforcement Network (FinCEN). (2014). *Advisory to U.S. Financial Institutions on Promoting a Culture of Compliance*.
[5]See Edmonds S. C. (2010). Accountability = Consequence Management.
[6]See US Department of Justice, Criminal Division, Fraud Section, *Evaluation of Corporate Compliance Programs*. (2018). 1–2.

AML/sanctions risks and weaknesses in the AML/sanctions risk management processes.[7]

Therefore, having a defined protocol for conduct investigations is a key component of an effective compliance risk management; it forms the basis for identification of misconduct, and, subsequently, remediating or correcting it. Formalizing the protocol provides transparency, consistency, and reliability in handling misconduct to staff and other stakeholders and ultimately protects the reputation of the financial institution.

3. Typology for Compliance Misconduct

A. Defining Misconduct

Before looking into the requirements for a protocol for performing conduct investigations, it is important to define what constitutes misconduct and to delineate it from other types of undesirable behavior in the workplace.

The two main categories to be differentiated are poor performance and misconduct:

On the one side, "Poor performance does not look at the behavior of the employee at work. (…) Poor performance looks at whether the job, which the employee is paid to do is being done properly."[8] Most companies have performance management systems in place. The objective of performance management in the workplace is to measure employees' performance in terms of quality and quantity against the set objectives, which are normally derived from or aligned with the organizational objectives.

Misconduct, on the other side, "occurs when a rule is broken or some other unacceptable behavior happens."[9] As misconduct in relation to AML/sanctions may also have legal implications, the following definition from Wikipedia is more fitting for this white paper: "In law, misconduct is wrongful, improper, or unlawful conduct motivated by premeditated or intentional purpose or by obstinate indifference to the consequences of one's acts."[10]

In the context of AML/sanctions, relevant rules may be external rules and regulations, such as the BSA/AML law or local and international sanctions regulations, or the financial institution's internal policies and procedures established to adhere to external laws or effectively implement its risk appetite (e.g., by business restrictions).

Poor performance is usually met with the tools of performance management. Misconduct needs to be identified, investigated, assessed, and sanctioned. These individual steps to be taken for each case of suspected misconduct are accompanied by reporting and quality assurance.

---

[7]See Bloch, 1.
[8]See Pangea Labour Solutions. (2015). *Difference between Misconduct and Poor Work Performance*.
[9]See Pangea Labour Solutions.
[10]See Wikipedia. *Misconduct*.

Before considering each of the phases for conduct investigations and the requirements for a formal corporate protocol for AML/sanctions-related breaches in sections 4 and 5 of this white paper, it is important to consider that misconduct can occur both at the employee as well as management level, or a combination of both. The next section looks at the different types and degrees of misconduct in more detail.

B. Employee Misconduct

At the level of the employee, misconduct can occur in different degrees, which are reflected in legal definitions, such as those of U.S. criminal law. The distinction is based on the motivation for the misconduct, and the level of awareness that the conduct is conflicting with external laws and regulations, the financial institution's internal policy and guidelines, or its corporate values.

The most severe level is misconduct performed knowingly and willfully. This relates to breaches, which are performed with the full knowledge and intention to deceive or mislead.[11] Examples are cases where implemented control mechanisms are actively circumvented in order to pursue business opportunities otherwise restricted or reducing application of risk-mitigating measures (e.g., manipulation of customers' AML risk scores by relationship manager).

The second level is misconduct performed knowingly. This refers to breaches where the conduct was performed "with knowledge that it was not correct." It requires knowledge and awareness of the facts or situation, but does not require the knowledge of the regulation governing the conduct.[12] For example, where requirements for CDD are not fully adhered to, but without benefit to the employee involved.

The third and last category is willful blindness. As the Association of Certified Anti-Money Laundering Specialists (ACAMS) states in its Study Guide for the CAMS Certification Examination: "Courts define 'willful blindness' as the 'deliberate avoidance of knowledge of the facts' or 'purposeful indifference.'" In AML cases, courts have held that willful blindness is the equivalent of actual knowledge (…).[13]

An example may be where there are obvious red flags for money laundering in the customer's transactional behavior that are not noticed and taken up by the relationship manager in the form of internal referral or escalation.

[11]See The United States Department of Justice (US DOJ) Criminal Resource Manual. *910 Knowingly and Willfully.*

[12]See US DOJ. *910 Knowingly and Willfully*.

[13]See Association of Certified Anti-Money Laundering Specialists (ACAMS). (2012). *Study Guide for the CAMS Certification Examination*, *5th ed.* 14–15.

C. Management Misconduct

While the general categories described in the previous section apply to all staff, and therefore include management, there also is the need to specifically consider the role of management in the misconduct.

This is shown in the U.S. Department of Justice's Guidance for Evaluation of Compliance Management, which asks: "Is there proper accountability as demonstrated for managers under whose watch misconduct occurred? Is the application of discipline consistent?"[14] While the guidance relates to fraud, this is equally relevant in AML/sanctions, where breaches may have legal and regulatory impacts for financial institutions, as well as leading to individual liability.

Thus, in any case where misconduct has been identified, in addition to establishing the facts and circumstances of the misconduct and the role of the employee, the role of management in the line above the employee has to be considered. The question to be answered is whether management had a role in facilitating or enabling the misconduct.

Just as with the employee, one criterion for differentiating the relevant management misconduct is the level of awareness and active involvement in the misconduct.

The most severe level is active and willful exertion of influence by management on the employee resulting in the misconduct. The second level is where steering of the management has led to the misconduct. While it is not necessarily required that the employee perform the breach, it resulted from the employee working towards the set targets and objectives.

The third category is lack of oversight by the management. In this respect, the definition of misconduct goes further than the definition cited above. While the underlying case may result from active wrongdoing of the employee, it may be neglect by the responsible line management that is classified as the misconduct on the management level.

D. Further Relevant Parties in the Misconduct

Looking at the relevant parties potentially involved in the misconduct, it is important to consider the control governance model in the financial institution. For the risk management of AML/sanctions in financial institutions, the established framework is the three lines of defense model.

Under the three lines of defense model, the operative units are the first line of defense. They are the risk owner, via the customer relationships they own and the transactions that are contracted and executed. The second line of defense is the risk control functions that set the standards based on the relevant laws and regulations and perform monitoring and surveillance activities. In relation to AML/sanctions, this

[14]The United States Department of Justice (US DOJ), Criminal Division, Fraud Section. (2017). *Evaluation of Corporate Compliance Programs.*

is the department supporting the AML/sanctions officer who is responsible, amongst others, for policies and guidelines, delivering training, performing transaction monitoring, and reporting to the board of managing directors. Last but not least, the internal audit function as third line of defense performs independent testing on the design appropriateness and operating effectiveness of the AML/sanctions risk management program.

Considering this division of work, as part of a conduct investigation, it is important to consider the potential role of all three lines of defense. This means that in a case where the breach has occurred in the business line of the financial institution, it needs to be verified whether this should or could have been identified by the compliance function, or the internal audit function of the financial institution, and whether the misconduct was facilitated by failure of these functions to properly perform the relevant activities.

In cases where the misconduct relates to the maintenance of customer relationships or executing transactions with AML/sanctions relevance, it needs to be established whether the AML/sanctions compliance function has reviewed or approved the customer relationship in the past, handled AML alerts or sanctions hits relating to the customer or customer's transactions correctly, or whether these should have come to their attention. In relation to the audit function, it should be evaluated whether audit covered the area appropriately, and if yes, whether it could or should have identified the misconduct or the process or control failures facilitating the misconduct.

Thus, the investigation should include all three lines of defense to obtain a holistic view about the facts and circumstances of the breach and who contributed to it.

4. Conduct Investigation Lifecycle

As conduct investigations are quite similar to the performance of an audit engagement, it may be appropriate to define the lifecycle of conduct investigations along the phases for a standard audit.

For audits, the Institute of Internal Auditors (IIA) in its Performance Standards defines seven phases:[15]

- Managing the Internal Audit Activity
- Nature of Work (Risk Management, Control, Governance)
- Engagement Planning
- Performing the Engagement
- Communicating Results
- Monitoring Progress
- Resolution of Management's Acceptance of Risk

As conduct investigations are triggered by ad hoc events, the Nature of Work corresponds to the identification of potential cases of misconduct. The Engagement Planning phase covers the decision about the need and value of initializing a conduct investigation, and consequently defining the scope. Performing the

[15]See IIA, 10–20.

engagement corresponds to performing the conduct investigation. Communicating results corresponds to Reporting. The last two phases, Monitoring Progress and Resolution of Management's Acceptance of Risk, are summarized under Follow-up.

The lifecycle of a conduct investigation for this white paper therefore is divided into the following five phases:

Managing the internal audit activity relates to the effective overall management of the activity to ensure it adds value to the organization.[16] As this is a general requirement for any corporate function, it will not be considered further in this white paper.

A. Identification of Potential Misconduct

The first step in detailing the sources for identification of potential cases of misconduct is to clearly define the scope for conduct investigations. For compliance-related misconduct, it has to be clearly defined which legal or regulatory areas (e.g., AML, sanctions, markets compliance, fraud…) are in scope, as this will have an impact on determining the relevant sources/functions where potential misconduct may be identified. Regardless of the organizational setup of the financial institution, the two functions that have to be considered at a minimum are the relevant compliance function and the internal audit function.

In relation to AML/sanctions, this would be the organization of the anti-money laundering/sanctions officer and the audit function. However, depending on the organizational structure, further functions may need to be considered, such as AML/sanctions officers in the business lines or functions responsible for the customer complaints or whistleblowing channels.

Once the relevant sources have been identified, each of these has to define trigger events for potential cases of misconduct.

For the AML/sanctions compliance function, these may be:
- Accumulation of customer relationships where due diligence requirements are not being met
- Accumulation of SARs in relation to customers of one relationship manager/branch
- Circumvention of business restrictions implementing the financial institution's risk appetite
- Circumvention of sanctions requirements
- Compliance testing with critical results in relation to AML/sanctions testing

For the audit function, trigger events in the context of regular audit engagements may be:

[16] See IIA, 10.

- Misconduct identified as root cause for either
    - Accumulation of AML/sanctions-related breaches/incidents
    - Significant single AML/sanctions-related breaches/incidents
- Overall audit result in relation to AML/sanctions below a certain level
- Significant structural deficiencies with regard to AML/sanctions-related processes and controls

In addition to defining the trigger events, it is also important to define a materiality level for the cases to be considered relevant for potential conduct investigation. Regulatory requirements, as well as the risk appetite of the financial institution, will be decisive factors.

At a minimum, the following cases should be considered significant:
- Data request/subpoena by law enforcement agency or regulatory authority
- Investigation by law enforcement agency or regulatory authority
- Fine/regulatory action against financial institution or employee
- Systematic/structural deficiencies/misconduct
- Critical results by internal (compliance/audit function) or external testing

The type of trigger event will also have an influence on whether employee and/or management misconduct have to be considered as relevant. In cases of systematic/structural deficiencies or critical results of internal or external testing, only management misconduct is relevant. In other cases, employee as well as management misconduct has to be considered.

Relevant potential cases of misconduct meeting the above criteria then need to be assessed in more detail. The assessment will be the basis to decide about the initiation of a formal conduct investigation.

B. Deciding on Conduct Investigations

Once a relevant case of potential misconduct has been identified, the next step is to assess the case and then decide about the initiation of a formal conduct investigation. The result of the assessment to a certain extent will also influence the scope and methodology for the investigation.

The assessment should be performed in a structured way to ensure that the assessment criteria are transparent and consistent across different cases. To balance the structured approach with the fact that each case will be unique, there should be the possibility to overwrite the pre-determined decision taking. However, it should be ensured that each deviation from the structured decision taking is justified and the rationale documented.

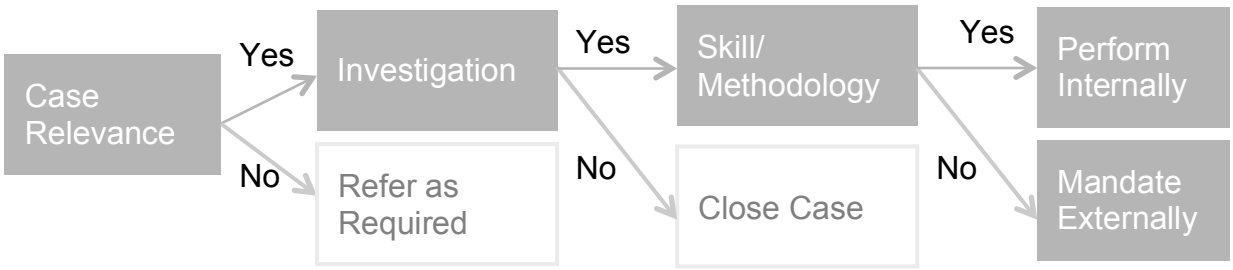
The assessment may be structured along the following criteria:

i. Case Relevance
   (Re-) Confirmation that the case under review meets the requirements for a conduct investigation based on scope and materiality
ii. Feasibility of Conduct Investigation

Assessment whether there are limitations to the investigation and whether it is due to yield additional knowledge and/or value

iii. Skill/Methodological Requirements
Analysis whether there are requirements in terms of skills and methodology that are not available in the firm and warrant mandating external support or performance of the investigation.

The assessment can be structured along a decision tree:



When the case relevance is denied for consideration of a formal conduct investigation, it is important to take into account that further action may be required and thus has to be referred accordingly. In circumstances were the feasibility, or value added, of the investigation is denied, the reasons have to be comprehensively documented; the same applies to the assessment with regard to the skill and methodology requirements.

All factors in relation to the assessment of cases have to be documented and stored.

C. Performing Conduct Investigations

The objective of the conduct investigation is to establish the facts and circumstances of the breach and then clarify the accountability. In order to meet the objectives, relevant data has to be obtained and analyzed.

Accordingly, the investigation process may be divided into three different phases:
1) Data collection
2) Fact finding
3) Forensic investigation

It should be noted that the phases are not distinct and may be performed overlapping, or in reiterations, depending on the progress and findings of the investigation.

To ensure compliance with applicable data privacy and co-determination law, this white paper proposes a phased approach to ensure that the requirements are met. It also has the benefit that there are defined checkpoints for deciding the continuation of the investigation, and requirements for the extension of data collection and the relevant approach. For each step, the data protection officer and employee representation body, as required, should be involved as early as possible and in a structured manner.

In jurisdictions with lesser requirements, this phased approach may also be considered by using the checkpoints to ensure that the continuation of the investigation is warranted under consideration of the gained knowledge and the further effort involved.

1) Data collection

The data collection phase is a critical step in any investigation. On the one hand, it forms the basis to obtain a complete picture on the facts and circumstances of the potential misconduct; and on the other hand, it is subject to data protection and co-determination requirements.

A conduct investigation in any area will involve collection and review of personalized data and should be subject to an assessment of the admissibility. The assessment, depending on the relevant jurisdictions, should consider, amongst others, the following topics:

- Data protection requirements in relation to processing employee data
- Information rights of the affected employee(s)
- Involvement of employee representation body (e.g., workers' council)

With respect to misconduct in the area of AML/sanctions, relevant sources of data will specifically comprise customer-related data, such as customer files including the know-your-customer (KYC) data, transactional data, and raised suspicious activity reports (SARs). In relation to SARs, even stricter requirements apply under the confidentiality provisions. While it is possible to use the information of the SARs internally, it needs to be considered that "FinCEN and the federal banking agencies take the position that a bank's internal controls for the filing of SARs should minimize the risks of disclosure."[17] Therefore, the need to use SAR data in the investigation and the risk of SAR disclosure need to be carefully taken into account. Where SAR data is processed or passed on to further parties in the context of an investigation, relevant safeguards protecting SAR confidentiality need to be implemented and documented.

2) Fact Finding

In the fact-finding phase, information around the potential misconduct is obtained. The key questions to be answered are:

- Did a breach occur?
- What were the circumstances of the breach?
- Does the breach constitute a violation of law and/or internal policy?

In AML/sanctions-related cases, data to be analyzed will relate to the customer relationship in question and related transactional data with the aim of establishing whether a breach has in fact been committed. Related data from the AML/sanctions compliance function is data on AML transaction-monitoring alerts, suspicious activity reports, sanctions hits, blocked funds, and further information relating to the customer relationship or relevant transactions. Furthermore, relevant policies and

[17]See Federal Financial Institution Examination Council (FFIEC). "Suspicious Activity Reporting Prohibition of SAR Disclosure." *Bank Secrecy Act Anti-Money Laundering Examination Manual.*

procedures, work instructions, and organizational information may need to be reviewed.

This stage of the investigation will also comprise fact-finding interviews. The aim is to obtain information about the policies and procedures effective and implemented at the time. Furthermore, interviews may also serve the aim to gather specific information surrounding the potential misconduct.

Once the misconduct has been confirmed, the next step is to establish the scale of the misconduct; i.e., to establish whether it is limited to the case(s) originally reported or has occurred on a wider scale. Thus, the scope of the review and data required may be extended to cover the full customer portfolio and related transactions and alerts of the employee(s) involved.

3) Forensic Investigation

Once the misconduct has been confirmed and the scale identified, this phase is about establishing the accountability for the misconduct and the severity of misconduct. The key questions to be answered are:

- Who committed the breach?
- Who was involved in and facilitated the breach?
- Who has, and who should have, identified the breach?

Data required in this stage usually concerns the communication data (email, chats, telephone recordings) and is the most critical under data protection and co-determination requirements. The data has to be clearly scoped and ring-fenced in terms of timeframe and persons involved, based on the findings of the previous phases.

In this phase, forensic interviews or interrogations will be held. In forensic interviews, staff directly or indirectly involved in the misconduct will be confronted with the findings of the investigation and questioned in terms of their awareness of, and motivation for, the misconduct. Especially in interviews where employees suspected of the misconduct are interviewed, special rules may apply depending on the jurisdiction. Special requirements range from information rights to the right to be accompanied, to the interview and time limits for disciplinary actions. It is therefore strongly recommended to involve the human resources and/or legal department.

D. Reporting

Once the investigation has been concluded, it is good practice to produce a report, which summarizes the investigation scope, approach, and results. The report and subsequent follow-up on the investigations findings is an important tool to achieve the objectives of conduct investigations.

For reports on conduct investigations, the corporate protocol should detail a minimum standard for the structure and the expected content. Furthermore, the addressees need to be defined.

A possible structure of a conduct investigation report may include, but is not limited to, the following:

- Background
- Scope of the investigation, including specific timeframe
- Investigation approach/methodology
- Results/key findings including follow-up/corrective actions

The key findings in most cases will consist of two types of results: conduct summaries and process findings. The objective of a conduct summary is to present the sequence of events for each involved/suspected employee separately. It will focus on the responsibility, knowledge, and actions of each individual potentially involved in the misconduct and link it with the evidence obtained. In many cases, presenting the conduct summary against a timeline is useful. The conduct summary will be the basis for the conclusion on the individual's accountability for the misconduct.

The process findings, just like findings from internal audit, will be the basis for improving risk management processes and controls, and are key in ensuring that weaknesses identified are remediated so that similar cases cannot occur again.

Last but not least, for the report, the appropriate report distribution has to be identified. In line with IIA standards, the criteria in identifying the recipients is that the recipients "ensure that the results are given due consideration."[18] Relevant addressees therefore are the parties responsible for evaluating and respectively sanctioning the conduct, as well as taking corrective actions to address process or control weaknesses. Considering the sensitivity of conduct investigations, the distribution needs to be carefully balanced between ensuring proper follow-up of the actions and the confidentiality of the matter. To consider this appropriately, separate and very limited distribution of the conduct summaries is recommended.

E. Follow-up Conduct Investigations

There must be formalized processes to follow up, to conclusion, both the results from the conduct summary and the process findings.

In relation to the evaluation of the conduct, the report should not offer recommendations regarding the sanctioning of involved employees or similar post-investigation activity.[19] That being said, however, there should be a clear protocol for referring this to the appropriate department or body in the financial institution and ensuring a structured and complete follow-up to the conduct component. Possible parties to decide about sanctioning may be an ethics committee, the responsible line management, human resources and legal department, or any combination. It is important that there is a clear and formalized protocol in the same way as for the conduct investigation process itself.

For the follow-up of process findings, the same standards as for audit findings should be applied. In line with the requirements of the IIA, the process findings from conduct

[18] See IIA, 19.
[19] See Bloch, 20.

investigation should be subject to a follow-up process to monitor and ensure that corrective actions are effectively implemented or that there is a formal risk acceptance.[20] Further requirements that should be covered in the protocol are regular reporting on the implementation status of process findings, as well as a defined escalation process in case corrective actions are not implemented timely or not at all.[21]

5. Managing Conduct Investigations - Standards and Governance

A. Standards for Performance of Conduct Investigations

As outlined in the previous section, conduct investigations have many similarities to audit engagements. Consequently, when looking at the standards for conduct investigations, it is appropriate to consider standards defined for workplace investigations as well as those defined for internal audit activities.

Outlining these two sets of standards in context shows that there is considerable overlap:

Workplace Investigations[22]	**Internal Audit[23]**
Confidentiality	*n/a (not covered)*
Preventing Retaliation	
Proper Mindset	Proficiency and Due Professional Care
Professionalism	
Competence	
Timeliness	
Independence	Independence and Objectivity
Objectivity and Impartiality	
N/a (not covered)	Purpose, Authority, and Responsibility
N/a (not covered)	Quality Assurance and Improvement Program

In the next section, this white paper provides an overview of the following three standards, which are most critical to safeguard the integrity of conduct investigations:

- Proficiency and Due Professional Care
- Independence and Objectivity
- Confidentiality

“Purpose, Authority and Responsibility” as well as “Quality Assurance and Improvement Program” will be covered in Section B, looking at governance considerations.

[20] See IIA, 20.
[21] See IIA, 20.
[22] See Bloch, 2–5.
[23] See IIA, 3–10.

1) Proficiency and Due Professional Care

Sufficiently qualifying staff for the respective role in the financial institution is a basic requirement, and is also required of any internal auditor. As the IIA standard states: "Individual auditors must possess the knowledge, skills, and other competencies needed to perform their individual responsibilities."[24] Due to the special nature and the potential legal implications, the quality of conduct investigations is at least as important. While the skills are in many ways similar to those of an auditor, there are further specific skills that need to be maintained in the function responsible for performing the investigations. On the one hand, the knowledge required relates to AML/sanctions requirements and the financial institution's policies and procedures. On the other hand, know-how on investigation techniques is required; most notably in the area of interviewing skills and gathering and documenting the evidence.[25] Last but not least, the investigations unit should also have knowledge of applicable labor, data protection, and co-determination laws.

In line with the stipulations of the IIA standards, not each investigator needs to possess the full range of skills and competencies, but rather, they need to be maintained by the function performing the investigations collectively.[26]

2) Independence and Objectivity

To maintain the integrity of any investigation, the independence of the staff involved in the entire investigation lifecycle is of paramount importance. In line with the standards for internal auditing,[27] both organizational and individual objectivity need to be considered.

Organizational independence is defined based on the reporting line of the executive responsible for the investigations and a regular (annual) formal confirmation to the board of the financial institution.[28] Organizational independence needs to be considered especially in allocating the responsibility in the organization for executing and steering conduct investigations and in setting up the reporting line to the board of the financial institution. The different options in allocating the responsibility for the performance of conduct investigations will be explored in the next chapter.

The second dimension to consider is individual independence. It is defined as the relevant staff having an impartial, unbiased attitude and avoiding any conflict of interest.[29] The interpretation defines a conflict of interest as "a situation in which (the person involved) has competing professional or personal interest. (…) A conflict of interest exists even if no unethical or improper act results." Individual independence in contrast to organizational independence has to be considered for each case of misconduct and for the individuals involved in each phase of the investigation lifecycle.

[24]See IIA, 6.
[25]See Bloch, 4.
[26]See IIA, 5.
[27]See IIA, 3–5.
[28]See IIA, 4.
[29]See IIA, 5.

Conflicts of interests can occur when the potential misconduct relates to, for example:

- the own field of work/responsibility;
- the field of work of a supervisor or manager in the direct line;
- a person to whom a close personal relationship exists; or
- a member of the financial institution's board of directors.

In order not to taint the integrity of the process, it is therefore recommended that the corporate protocol for each phase comprises a checkpoint to verify that there are no conflicts of interest, neither on an organizational nor personal level, for the individuals involved in the process.

3) Confidentiality

A third aspect that is critical for conduct investigations is to maintain confidentiality. There may be serious consequences on the investigation, individuals affected by the investigation, and the financial institution if confidentiality is not maintained. Confidentiality needs to be maintained throughout the entire investigation process from the receipt of the information of the potential AML/sanctions-related misconduct through to the end of the investigation and beyond it.[30]

Confidentiality is also specifically important to prevent retaliation. Anyone reporting a potential misconduct and being involved in the investigation, either as interviewee or investigator, must be protected from detrimental consequences.[31]

B. Governance Considerations for Conduct Investigations

One of the key questions looking at the governance for conduct investigations is the question: to which function the responsibility for performing conduct investigations in the area of AML/sanctions should be allocated. This white paper will discuss three options and their synergies, advantages, and disadvantages.

Option 1: Allocation to the AML/Sanctions Compliance Function

Looking at the subject matter of the potential misconduct, allocating the responsibility to the AML/sanctions compliance function may be the first option to come to mind. Staff in this area have the in-depth knowledge about the legal and regulatory requirements as well as the internal policies and processes. In fact, in many cases, the organization of the AML/sanctions department will have identified the potential misconduct as part of its surveillance and monitoring responsibility or have been informed about it by the first line of defense.

While there are no professional standards, such as for the internal audit function, the requirements on the AML/sanctions compliance department cover similar areas; confidentiality is required in context of the non-disclosure of SAR requirement.[32]

[30] See Bloch, 4.
[31] See Bloch, 5.
[32] See Comptroller of the Currency. (2010), *Code of Federal Regulations*, 12 CFR Part 21 – Section 21.11(k) Confidentiality of SARs.

Appropriateness of qualitative and quantitative staffing has to be ensured for the organization supporting the AML officer and reported on as part of the regular (at least) annual reporting. Last but not least, the AML compliance officer should be free of conflicts of interest.[33] In many jurisdictions, this is supported by the requirement for the AML compliance officer to have a direct reporting line to the board of managing directors.

On the other hand, in looking at the parties that may need to be considered in conduct investigations as described in Section 3.D. of this white paper, it may often be the case that the role and handling of inquiries or transactions by the AML/sanctions department needs to be looked at as part of the investigation. Here, the independence and objectivity throughout the investigation lifecycle may be tainted, and this will need to be addressed as part of the corporate protocol. Furthermore, some of the specific skills required for conduct investigations will need to be specifically obtained.

Option 2: Allocation to the Audit Function

As we have seen in looking at the standards for performing conduct investigations, there is a lot of overlap with the standards for internal audit functions. If the internal audit function is established in line with the professional standards of the IIA, organizational independence, including a direct reporting line to the board, objectivity, and professional due care and diligence are warranted. Specifically, the area responsible for AML and sanctions will also possess the required knowledge in the area of regulations and the financial institution's policies, processes, and controls.

However, there are two aspects that potentially need to be compensated for. First, the objectivity of the audit function may be compromised in considering the role of the internal audit function itself in the potential misconduct. This is the case even more so when—based on the subject matter expertise—the audit department assessing AML/sanctions compliance is tasked with performing conduct investigations. Second, there must be special rules and procedures for performing quality assurance and maintaining an improvement program. Under the three lines of defense model, there is no further independent party in the financial institution that may perform independent assessments. Consequently, regular external assessments of the procedures and work performed should be mandated and performed.

Option 3: Allocation to another/separate investigation function in the financial institution

Looking at the downsides of the first two options in regard to ensuring objectivity and covering the responsibilities across all potentially involved functions in the context of the three lines of defense model, allocation to another function outside the AML/sanctions function or internal audit function may be an alternative. In any case, responsibility should be assigned to a second line function, which reports to a different member of the management board than the business lines and the

[33]See FFIEC. BSA Compliance Officer.

AML/sanctions compliance function. One option may be setting up a specialized investigation function covering any kind of misconduct (including, for example, general misconduct, fraud, and compliance-related) in the financial institution. This function would then focus on the investigation techniques (especially forensic data analysis and interviews) and expertise in the applicable data protection and labor law requirements. While this option may address the independence of the investigation and the specific skill requirements, the challenge in this set-up is to maintain the expertise around AML/sanctions requirements and the implemented control environment.

As can be seen from the discussion of the three options above, there is not the ONE function in the financial institution where to allocate the responsibility for conduct investigations. Rather, the organizational specifics of the financial institution need to be considered, and any potential impediments compensated appropriately.

The outline of the investigation process has shown that there are many specific requirements that warrant consultation with the AML/sanctions compliance function as well as human resources and the legal department. As part of the governance, it may be effective to establish a decision board or standing committee supporting and monitoring the entire investigation process from the assessment and decision on whether to conduct an investigation to the follow-up. This may also support the objectivity throughout the process, under the condition that the independence and objectivity of the members is verified throughout the process.

Regardless of where the investigation responsibility is allocated in the financial institution, it needs to be ensured that the requirements of Purpose, Authority, and Responsibility, as well as Quality Assurance, are being met.

“Purpose, Authority, and Responsibility” means that for the responsible unit, “the purpose, authority and responsibility […] are formally defined.” It is recommended to include the relevant governance aspects, such as the position within the financial institution, the reporting/escalation line to the board, information rights and the key standards independence, objectivity, as well as proficiency and due professional care[34] in the charter or business objective of the unit.

Quality Assurance relates to the implementation of a quality assurance and improvement program designed to enable an evaluation of the investigation function for its conformance with the internal standards as well as with compliance with relevant external laws. Where the responsibility is allocated to a second line function in the financial institution, the internal audit function should include the investigation function in its audit plan, and thus may be one component of the quality assurance program. It may be further considered to perform additional external assessments to complete the program.[35]

In cases where there is no solution for the allocation of responsibility that ensures meeting the requirements, as a last resort, there remains the possibility to mandate the investigation externally. However, the decision of who in the financial institution

[34]See IIA, 3.
[35]See IIA, 7–9.

steers the external investigation needs to be carefully considered to ensure that objectivity and independence are not tainted.

6. Conclusion

Over the last years, a culture of compliance has been identified as an important component for the effective management of AML/sanctions risks.

A culture of compliance consists of communicating the expectations on compliance with the applicable laws, regulations, and internal requirements, but it also requires processes to identify and handle cases of non-compliance. This is particularly important in order to create accountability and learn from errors.

In the area of AML/sanctions, breaches may have severe consequences on the financial institution as well as on individuals involved. Consequently, there is a need, and regulatory expectation, to investigate these if they occur. Therefore, having a formalized protocol for investigating potential cases of misconduct is a matter of transparency and consistency, as well as an important cornerstone for the compliance culture of the financial institution.

Investigating potential cases of misconduct is a critical process for all parties involved—informants, employees involved in the suspected misconduct, and the financial institution as a whole. In addition to the relevant AML/ sanctions laws and regulations that have potentially been compromised, the investigation process is also impacted by data protection, labor law, and co-determination requirements.

These need to be considered in a formal protocol, which defines the process from the identification of potential cases of misconduct to the conclusion of the follow-up actions identified as result of the investigation.

Due to the criticality of the investigations, it is important to establish standards and carefully consider the governance around the assignment and set-up of responsibility for investigating AML/sanctions-related misconduct.

This white paper has considered standards for workplace investigations in combination with the role of, and standards for, the AML/sanctions compliance function and the internal audit function. On this basis, a sample process approach, standards, and possible governance models have been developed and outlined.

Considering these standards in corporate protocol will provide transparency on, and safeguard, the integrity of the investigation process and thus protect the reputation of the financial institution. As Bloch states, "…how companies investigate potential misconduct can affect that company's reputation almost as much as the alleged conduct itself."[36]

[36]See Bloch, M. C. (2008). *Guide to Conducting Workplace Investigations*. 1.

7. References

Association of Certified Money Laundering Specialists (ACAMS). (2012). S*tudy Guide for the CAMS Certification Examination, 5th ed*.

Bloch, M. C. (2008). *Guide to Conducting Workplace Investigations*. Retrieved from: http://www.corporatecompliance.org/Portals/1/Users/169/29/60329/Workplace_Investigations_Guide.pdf.

Comptroller of the Currency. (3 December 2010), *Code of Federal Regulations*, 12 CFR Part 21 – Confidentiality of Suspicious Activity Report. Retrieved from: https://www.govinfo.gov/content/pkg/FR-2010-12-03/pdf/2010-29880.pdf

Edmonds, S. C. (7 May 2010). *Accountability = Consequence Management*. Retrieved from: https://www.drivingresultsthroughculture.com/2010/05/07/accountability-consequence-management/.

Federal Financial Institution Examination Council (FFIEC). *Bank Secrecy Act Anti-Money Laundering Examination Manual.* Retrieved from: https://www.ffiec.gov/bsa_aml_infobase/pages_manual/manual_online.htm. Now accessible under: https://bsaaml.ffiec.gov/manual.

Financial Action Task Force. (June 2007). *Guidance on the Risk-Based Approach to Combating Money Laundering and Terrorist Financing. High Level Principles and Procedures.* Retrieved from: https://www.fatf-gafi.org/media/fatf/documents/reports/High Level Principles and Procedures.pdf.

Financial Crimes Enforcement Network (FinCEN). (11 August 2014). *Advisory to U.S. Financial Institutions on Promoting a Culture of Compliance*. Retrieved from: https://www.fincen.gov/resources/advisories/fincen-advisory-fin-2014-a007.

Moskow-Schnoll, B. (1 November 2018). *Practical Tips for Ensuring Your AML Program Withstands the Scrutiny of Regulators*. Retrieved from: https://www.moneylaunderingnews.com/2018/11/practical-tips-for-ensuring-your-aml-program-withstands-the-scrutiny-of-regulators/.

Pangea Labour Solutions. (21 May 2015). *Difference between Misconduct and Poor Work Performance.* Retrieved from: https://www.linkedin.com/pulse/difference-between-misconduct-poor-work-performance-jj-s-solutions.

The Institute of Internal Auditors (IIA). (October 2016). *International Standards for the Practice of Internal Auditing (Standards)*. Retrieved from: https://na.theiia.org/standards-guidance/Public Documents/IPPF-Standards-2017.pdf.

The United States Department of Justice (US DOJ). 910 Knowingly and Willfully. *Criminal Ressource Manual*. Retrieved from: https://www.justice.gov/jm/criminal-resource-manual-910-knowingly-and-willfully.

The United States Department of Justice (US DOJ), Criminal Division, Fraud Section. (8 February 2017). *Evaluation of Corporate Compliance Programs.* Retrieved from: https://www.justice.gov/criminal-fraud/page/file/937501/download. (Updated April 2019)

Shasky Calvery, Jennifer. (30 January 2014). Remarks of Jennifer Shasky Calvery, Director Financial Crimes Enforcement Network. Retrieved from: http://fincen.gov/news_room/speech/html/20140130.html. Now accessible under: https://www.fincen.gov/news/speeches/remarks-jennifer-shasky-calvery-director-financial-crimes-enforcement-network-8.

Wikipedia. *Misconduct*. Retrieved from: *https://en.wikipedia.org/wiki/Misconduct*.